

ESET Cloud Office Security

Guía para el usuario

[Haga clic aquí para mostrar la versión de ayuda de este documento](#)

Copyright ©2023 de ESET, spol. s r.o.

ESET Cloud Office Security ha sido desarrollado por ESET, spol. s r.o.

Para obtener más información, visite <https://www.eset.com>.

Todos los derechos reservados. Ninguna parte de esta documentación podrá reproducirse, almacenarse en un sistema de recuperación o transmitirse en forma o modo alguno, ya sea por medios electrónicos, mecánicos, fotocopia, grabación, escaneo o cualquier otro medio sin la autorización por escrito del autor.

ESET, spol. s r.o. se reserva el derecho de modificar cualquier parte del software de la aplicación sin previo aviso.

Soporte técnico: <https://support.eset.com>

REV. 20/12/2023

1 Información general	1
1.1 Características clave	2
1.2 Novedades	5
1.3 Integración	6
2 Características técnicas	6
2.1 Requisitos	7
2.2 Planes compatibles con Microsoft 365	7
2.3 Planes de Google Workspace compatibles	8
2.4 Navegadores web compatibles	8
2.5 Política de retención de datos y limitaciones	9
3 Licencia para ESET Cloud Office Security	10
3.1 ESET Business Account	11
3.1 Crear una nueva cuenta de ESET Business Account	11
3.1 Agregar licencia de ESET Cloud Office Security en ESET Business Account	12
3.1 Administrar ESET Business Account	12
3.2 ESET MSP Administrator	13
4 Activar ESET Cloud Office Security	14
4.1 Desactivar ESET Cloud Office Security	16
5 Administrar los inquilinos en Configuración	17
5.1 Agregar su primer inquilino	19
5.2 Inquilino de Microsoft 365	21
5.3 Inquilino de Google Workspace	24
5.4 Quitar inquilino de ESET Cloud Office Security	30
5.5 Eliminar ESET Cloud Office Security del portal de Azure	31
6 Navegue por el ESET Cloud Office Security	31
7 ESET LiveGuard Advanced	33
8 Dashboard	34
9 Usuarios	36
10 Equipos y sitios	37
11 Detecciones	38
12 Informes	40
13 Cuarentena	42
14 Registros de la exploración	44
15 Políticas	45
15.1 Configuración de la protección para Exchange Online	48
15.2 Configuración de la protección de Gmail	51
15.3 Configuración de la protección para OneDrive	54
15.4 Configuración de la protección para Google Drive	55
15.5 Configuración de la protección para grupos del equipo	56
15.6 Configuración de la protección para sitios de SharePoint	57
15.7 Configuración de la protección de ESET LiveGuard Advanced	58
15.8 Informes y protección del aprendizaje automático	59
16 Administración de licencias	61
16.1 Acceso de usuario de ESET Cloud Office Security a una empresa concreta	63
17 Registro de auditoría	64
18 Enviar comentarios	65
19 Soporte técnico	65
20 Disponibilidad del servicio	66

20.1 Seguridad para ESET Cloud Office Security	66
20.2 Términos de uso	70
20.2 Acuerdo de licencia de usuario final	75
20.2 Contrato de procesamiento de datos	81
20.2 Cláusulas contractuales estándar	83
20.3 Política de privacidad	107

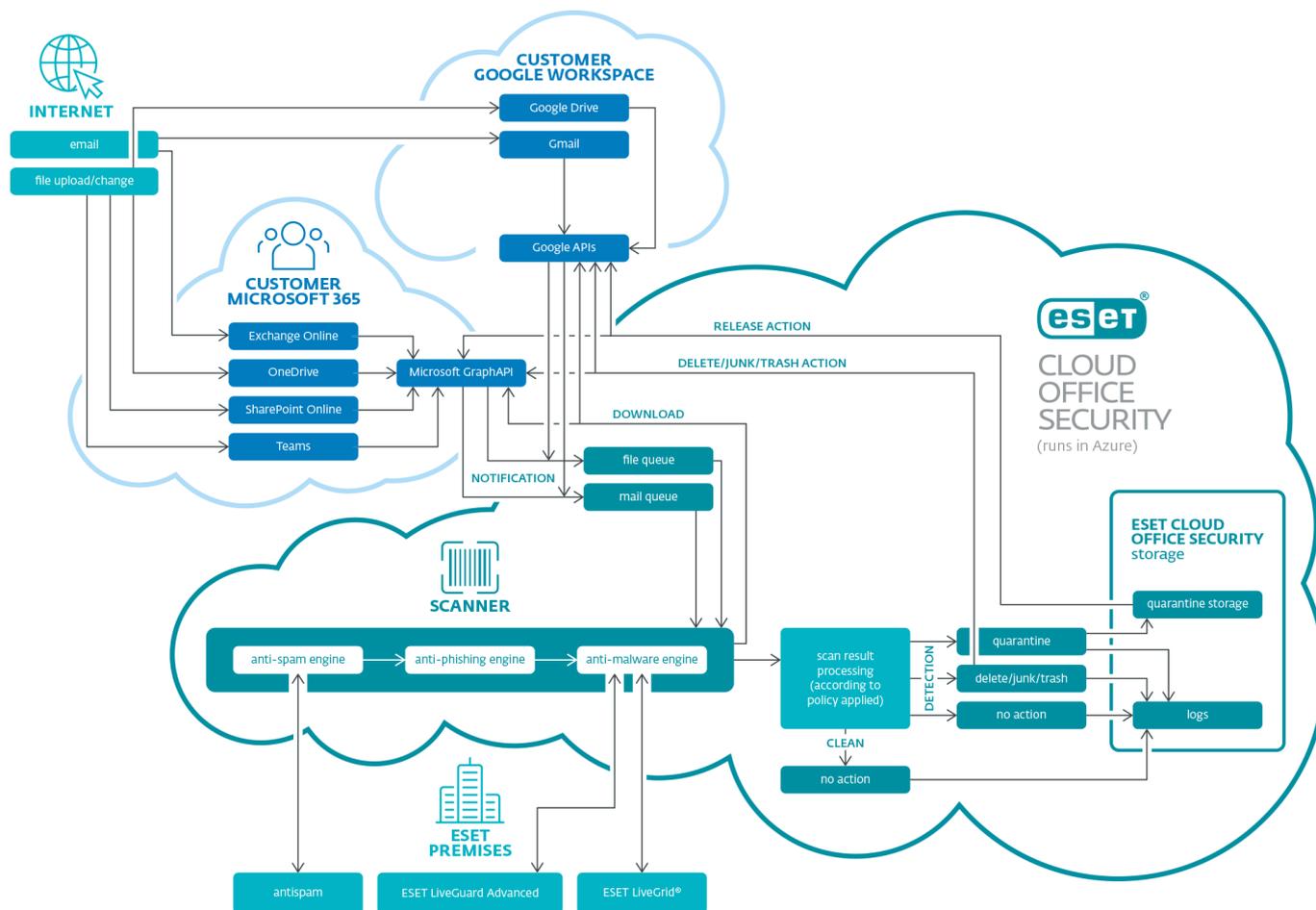
Información general

ESET Cloud Office Security es un servicio de nube escalable y de varios inquilinos en Microsoft Azure. ESET Cloud Office Security se ofrece como un producto Software-as-a-Service (SaaS) que opera por completo en la nube sin la necesidad de hardware. La más reciente combinación de filtrado de spam, exploración de protección contra malware y protección anti-phishing ayuda a proteger las comunicaciones de su empresa contra malware, minimiza los efectos negativos de los mensajes no solicitados en la productividad diaria y ayuda a evitar que los correos electrónicos externos entrantes se usen como canal para ataques dirigidos.

Los servicios de seguridad de ESET Cloud Office Security cubren los principales proveedores de plataformas en la nube y ofrecen una protección integral del correo electrónico con motores de protección contra malware de última generación y ESET LiveGuard Advanced. Esta solución ofrece una defensa avanzada contra amenazas mediante sandboxing basado en la nube, ya que analiza muestras sospechosas en un entorno aislado.

La arquitectura de ESET Cloud Office Security le permite iniciar la protección rápidamente conectándose a su plataforma en la nube: Microsoft 365 y Google Workspace. Le da el poder de administrar la protección a través de una consola basada en la web accesible desde cualquier lugar.

ESET Cloud Office Security proporciona protección preventiva avanzada para proteger las aplicaciones de Microsoft 365 de su empresa: Exchange Online, OneDrive, SharePoint Online y Teams. La misma protección se proporciona a las aplicaciones de Google Workspace: Gmail y Google Drive.



ESET Cloud Office Security protege OneDrive y el buzón de correo de los usuarios con licencia, así como los grupos del equipo y los sitios de SharePoint. Cada almacén de estas aplicaciones de Microsoft 365 está protegido, sin importar quién cargo un archivo o quién envió un correo electrónico. El contenido en sí está protegido, sea cual sea el autor. El autor también puede ser un usuario invitado para garantizar la mejor protección posible.

Características clave

La siguiente tabla contiene una lista de funciones disponibles en ESET Cloud Office Security.

Multi-inquilino	Puede proteger y administrar múltiples inquilinos de Microsoft 365 y Google Workspace desde una sola consola de ESET Cloud Office Security. Azure Active Directory (Azure AD) organiza los objetos, como usuarios y aplicaciones, en grupos llamados inquilinos. Los inquilinos le permiten definir políticas sobre los usuarios y aplicaciones de su organización para cumplir con las políticas de seguridad y operativas.
-----------------	--

Antispam	El Antispam es un componente esencial para cualquier servidor de correo. ESET Cloud Office Security usa un motor antispam de avanzada que previene intentos de spam y phishing con tasas muy altas de captura. ESET Cloud Office Security ha ganado consecutivamente la evaluación de filtro de spam por Virus Bulletin, una autoridad examinadora de seguridad líder, y ha recibido la certificación VBSpm+ por varios años. El motor antispam ha alcanzado un resultado de una tasa de captura de spam del 99,99% con cero falsos positivos, lo que lo convierte en la tecnología líder de la industria en la protección contra el spam. ESET Cloud Office Security El antispam se basa en la nube y la mayoría de las bases de datos en la nube están ubicadas en los centros de datos de ESET. Los servicios antispam en la nube permiten actualizaciones rápidas de datos que proporcionan un tiempo de reacción más rápido cuando surge un nuevo spam.
Protección contra phishing	Esta función evita que los usuarios accedan a páginas web conocidas por phishing. Mensajes de correo electrónico que pudieran contener enlaces que conducen a páginas web con phishing, ESET Cloud Office Security usa un analizador que busca en el cuerpo del mensaje y asunto de los mensajes de correo electrónico entrantes para identificar dichos vínculos (URL). Los vínculos se comparan con una base de datos de phishing que se actualiza continuamente.
Protección contra malware	Al ser una defensa innovadora y galardonada contra el malware, esta tecnología de punta evita ataques. Elimina todos los tipos de amenazas, incluidos los virus, ransomware, rootkits, gusanos y spyware con un análisis impulsado por la nube para mejores tasas de detección. Al tener una pequeña huella, es ligero en los recursos del sistema y no compromete su rendimiento. La detección contra malware usa un modelo de seguridad por capas. Cada capa o fase tiene varias tecnologías núcleo. La fase de pre-ejecución incluye las siguientes tecnologías: Explorador UEFI (Unified Extensible Firmware Interface), la Protección contra ataques de red, Reputación y Caché, Sandbox en el producto, Detección de ADN. Las tecnologías en la fase de Ejecución son el bloqueador de exploits, la protección contra ransomware, el explorador de memoria avanzado y el explorador de script (AMSI). La fase de Post-ejecución usa la protección contra botnets, el sistema de protección contra el malware en la nube y Sandboxing. Este conjunto completo de tecnologías núcleo proporciona un nivel de protección inigualable.
Políticas	Las organizaciones más grandes suelen tener múltiples departamentos y quieren configurar distintos ajustes de protección para cada unidad organizacional. ESET Cloud Office Security ofrece ajustes de protección basados en políticas, que se pueden asignar a inquilinos, usuarios, grupos del equipo o sitios de SharePoint seleccionados. Puede personalizar las políticas según sus necesidades.
Administrador de cuarentena	Inspecciona los objetos en cuarentena y lleva a cabo una acción adecuada (descargar, eliminar o liberar). Esta función ofrece una administración sencilla de los mensajes de correo electrónico, de los archivos adjuntos, así como de los archivos de Exchange Online/OneDrive/grupos del equipo/sitios de SharePoint que ESET Cloud Office Security ha puesto en cuarentena. La descarga le permite analizar los objetos puestos en cuarentena con herramientas de terceros, en caso de ser necesario, que pueden ayudarlo a decidir qué acción realizar.
Dashboard con estadísticas de detección	Acceda a una breve descripción general de las actividades de seguridad de Microsoft 365. El Dashboard aporta información básica en cada una de las pestañas de información general (Exchange Online/OneDrive/grupos del equipo/sitios de SharePoint). En la descripción general del usuario, se muestran la cantidad de inquilinos y el uso de licencias, así como las estadísticas por cada inquilino, es decir, cantidad de usuarios, principales destinatarios de spam/phishing/malware, principales cuentas sospechosas de OneDrive, principales grupos sospechosos del equipo y sitios de SharePoint. Puede elegir un período de tiempo y un inquilino en función de los cuales mostrar las estadísticas. En las pestañas de información general Exchange Online, OneDrive, grupos del equipo y sitios de SharePoint se pueden ver más estadísticas de detección y gráficos. Estas son estadísticas, como la cantidad de correos electrónicos y archivos explorados, y la cantidad de spam/phishing/malware detectados. En los gráficos se muestra el tráfico para cada tipo de detección: spam, malware y phishing.

<p>Detecciones con opciones de filtrado</p>	<p>Esta característica contiene todos los registros de detecciones. Los registros incluyen registros de todas las detecciones por análisis del correo electrónico en la pestaña Exchange Online y análisis de archivos en las pestañas OneDrive/grupos del equipo/sitios de SharePoint. Esto permite filtrar y encontrar de forma eficaz lo que busca utilizando información adicional sobre la detección específica (por ejemplo, un nombre de la amenaza, hash del archivo).</p>
<p>Usuarios</p>	<p>La entidad central que protege ESET Cloud Office Security es la cuenta del usuario. Para buscar información de utilidad, abra los Detalles de un usuario, como descripción general, configuración definida por políticas, lista de políticas asignadas al usuario y detecciones para Exchange Online y OneDrive. Esta función resulta útil cuando necesita investigar detecciones relacionadas con un usuario específico. También puede elegir qué usuarios desea proteger. Los usuarios se clasifican en grupos. Cada grupo es un inquilino de Microsoft 365 que contiene sus usuarios. Para simplificar la búsqueda de un usuario específico dentro de un grupo, filtre con múltiples criterios.</p>
<p>Informes y protección del aprendizaje automático</p>	<p>El aprendizaje automático avanzado ahora forma parte del motor de detección como una capa de protección avanzada, lo que permite mejorar la detección en función del aprendizaje automático. Lea más sobre este tipo de protección en el glosario. Puede configurar los Niveles de informes para las siguientes categorías: Malware, Aplicaciones potencialmente no deseadas (PUA), Aplicaciones potencialmente sospechosas y Aplicaciones potencialmente no seguras.</p>
<p>Informes (cuarentena de correo y estadística)</p>	<p>Reciba datos estadísticos para grupos de Exchange Online, OneDrive y Grupos del equipo, y sitios de SharePoint por correo electrónico, o genere y descargue un informe para el momento elegido. Puede programar informes para que se generen y distribuyan regularmente a los destinatarios de correo electrónico especificados. Elija PDF o CSV como formato de salida. Los informes contienen datos como el número de correos electrónicos analizados, así como malware, phishing y spam detectados. El formato PDF incluye datos mostrados en gráficos. Hay un gráfico para cada uno: correos electrónicos analizados, tráfico de malware, tráfico de phishing y tráfico de spam. También contiene estadísticas separadas sobre los principales destinatarios de cada categoría: malware, phishing y spam. Hay varias opciones disponibles para generar informes. Además, puede enviar a los destinatarios seleccionados un informe de Cuarentena de correo: una lista de los mensajes de correo electrónico puestos en cuarentena. El informe de la Cuarentena de correo se envía en la fecha y hora especificadas, pero solo si hay elementos nuevos que se deben informar.</p>
<p>Equipos y sitios</p>	<p>ESET Cloud Office Security ofrece protección para grupos del equipo o sitios de SharePoint. De esta forma, se amplía la protección a las soluciones de colaboración Microsoft 365 mediante la protección de SharePoint y equipos que admite el uso compartido de archivos de forma segura. Si ha estado usando ESET Cloud Office Security, es posible que se le pida que actualice el consentimiento antes de usar Equipos y Sitios.</p>
<p>ESET LiveGuard Advanced</p>	<p>Una capa de protección adicional contra amenazas avanzadas del día cero. ESET LiveGuard Advanced es una solución sandboxing basada en la nube que analiza los archivos enviados mediante la ejecución de un código sospechoso en un entorno aislado para evaluar su comportamiento. ESET Cloud Office Security envía archivos adjuntos de correo electrónico sospechosos y archivos de Exchange Online, OneDrive, Grupos del equipo y sitios de SharePoint a ESET LiveGuard Advanced para su análisis. Habilite y configure la función ESET LiveGuard Advanced mediante políticas. Los resultados del análisis se muestran en los Registros de la exploración.</p>
<p>Registro de auditoría</p>	<p>El registro de auditoría permite al administrador inspeccionar las actividades realizadas en ESET Cloud Office Security. Esta función puede resultar útil, especialmente cuando tiene varios usuarios de la consola ESET Cloud Office Security. Los historiales del registro de auditoría demuestran las actividades y muestran la secuencia en la que se produjeron. Los registros de auditoría almacenan información sobre la operación o el suceso específicos. Los registros de auditoría se crean siempre que se crea o modifica un objeto de ESET Cloud Office Security (grupo de licencias, usuario, política, informe, elemento de cuarentena, como archivo adjunto).</p>

Google Workspace (protección de Gmail y Google Drive)	ESET Cloud Office Security amplía la cobertura de servicios de seguridad a otro proveedor líder de correo electrónico en la nube, Google Workspace . ESET Cloud Office Security brinda protección integral a los usuarios de Gmail y Google Drive mediante el uso de todas sus características. Mantiene a los usuarios de Google Workspace a salvo del malware, el phishing y el spam.
---	---

Novedades

Información sobre las nuevas funciones y mejoras implementadas en cada una de las versiones de ESET Cloud Office Security:

↗ [Versión 353 del portal](#) publicada el 23 de noviembre de 2023

- Integración con [Google Workspace](#) añadida.
- [Navegador de productos](#) para acceder rápidamente a ESET Business Account (más consolas en los próximos meses).
- *Otras correcciones de errores y mejoras de back-end.*

↗ [Versión 342.3 del portal](#) publicada el 24 de octubre de 2023

- Se agregó la verificación de la cuenta de administrador de [Google Workspace](#).
- Se agregó la columna Tipo de [usuario](#).
- *Otras correcciones de errores y mejoras de back-end.*

↗ [Versión 311.2 del portal](#) publicado el 31 de julio de 2023

- Se agregó [Google Workspace](#) (protección de Gmail y Google Drive): acceda a las [funciones de vista previa](#) desde los enlaces rápidos.
- Tema [modo oscuro](#) añadido.
- Se agregó Navegador de productos para usuarios de acceso anticipado de ESET HUB.
- *Otras correcciones de errores y mejoras de back-end.*

↗ [Versión 293.7 del portal](#) publicado el 13 de julio de 2023

- Se agregó la asociación de inquilinos a los sitios de ESET Business Account (EBA). Este cambio garantiza la compatibilidad con el futuro portal de clientes ESET PROTECT HUB, que sustituirá a [ESET MSP Administrator](#) (EMA) y a [ESET Business Account](#) (EBA). Afecta solo a los clientes que usan licencias de varios sitios para proteger a un solo inquilino. Si este es su caso, se le pedirá que asocie a sus inquilinos con sitios de EBA.
- Se realizaron otras correcciones de errores y mejoras secundarias.

↗ [Versión 251.1 del portal](#) publicado el 21 de marzo de 2023

- Mejoras en la carga diferida de pantallas para ofrecer un mejor soporte a los inquilinos con decenas de miles de usuarios.
- Cambios en el asistente para [agregar inquilinos](#).
- Actualizaciones en la página Acerca de.
- Actualizaciones de los Términos de uso y la Política de privacidad ([Política de retención de datos y limitaciones](#)).

↗ [Versión 205 del portal](#) publicada el 9 de noviembre de 2022

- Se agregó una ventana de Novedades que aparecerá la primera vez que inicie sesión en la consola ESET Cloud Office Security. En esta ventana, se describen las características agregadas recientemente.
- Opción para exportar [Registros de la exploración](#) y [Registro de auditoría](#) a un archivo en formato CSV.
- Se agregó un nuevo ajuste al [Fusionar las políticas](#) con listas y correos electrónicos de notificación.

↗ [Versión 180.2 del portal](#) publicado el 27 de julio de 2022

- La nueva característica de [registro de auditoría](#).
- Cambie la sección Registros a Registro de la exploración.

↗ [Versión 156.2 del portal](#) publicado el 26 de abril de 2022

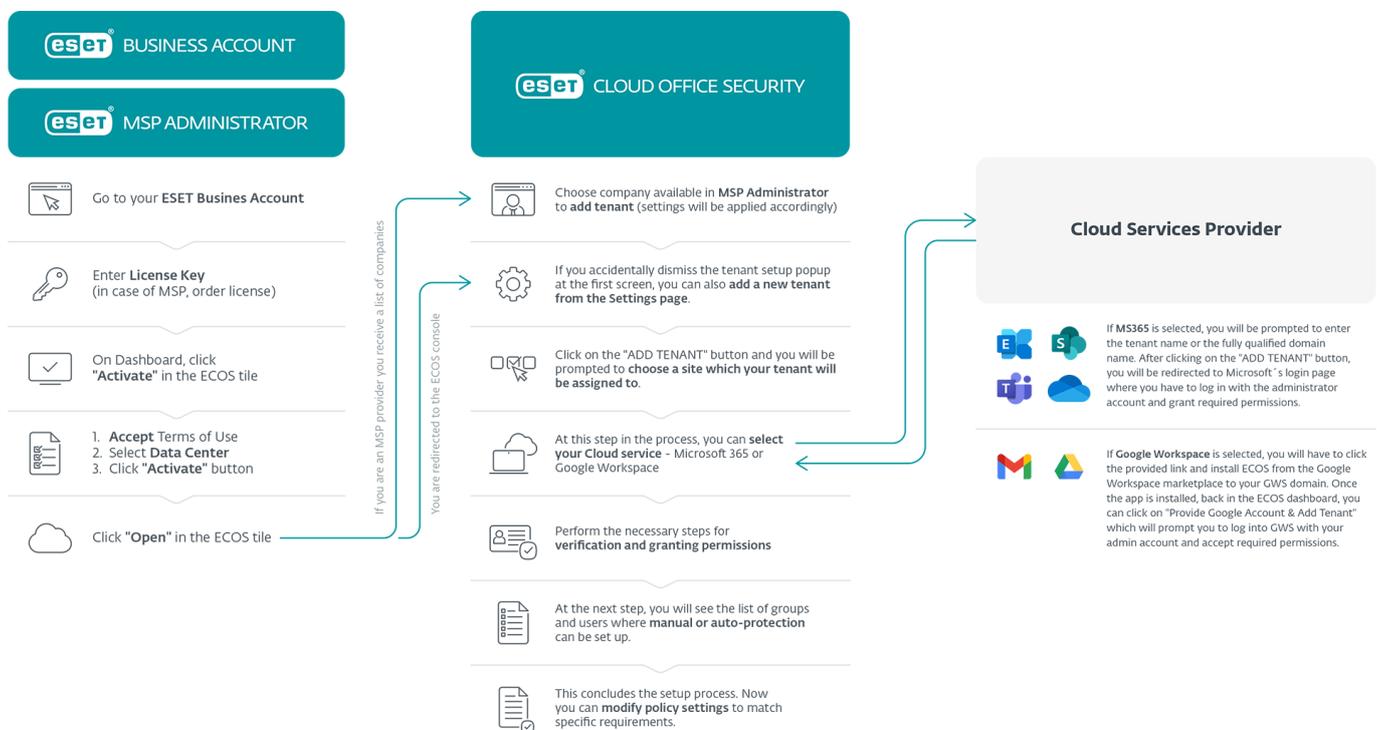
- Se ha cambiado el nombre de Dynamic Threat Defense a ESET LiveGuard Advanced.
- Envío de muestras de falso positivo/falso negativo para analizar.
- Listas de importación/exportación aprobadas, bloqueadas e ignoradas en [Políticas](#).
- En el dashboard, se muestra el recuento de usuarios no protegidos en la [pestaña Información general](#).
- Se ha corregido un error que ponía en cuarentena los correos electrónicos de notificación.

^ [Versión 140.6 del portal](#) publicada el 9 de febrero de 2022

- Capacidad de [informes de etiqueta blanca](#) (solo marca compartida o logotipo personalizado).
- Opción para definir el idioma preferido del correo electrónico de notificación ([notificaciones del propietario del buzón de correo](#)).
- Opción para definir el idioma preferido de las notificaciones [por correo electrónico de los miembros del inquilino](#).
- Filtrar correos electrónicos por ID del mensaje.

Integración

El flujo de integración de ESET Cloud Office Security con su proveedor de servicios en la nube:



Características técnicas

Características técnicas de referencia para ESET Cloud Office Security:

- [Requisitos](#)

- [Planes compatibles con Microsoft 365](#)
- [Planes de Google Workspace compatibles](#)
- [Navegadores web compatibles](#)
- [Política de retención de datos y limitaciones](#)

Requisitos

Para aprovechar el servicio de ESET Cloud Office Security que protege a si Microsoft 365, se requiere lo siguiente:

- [Plan de suscripción compatible con Microsoft 365](#)
- Acceso de administrador a Azure Active Directory (Azure AD)
- Azure Cloud Services: Exchange | OneDrive
- Una cuenta en el portal de [ESET Business Account](#) o [ESET MSP Administrator](#)

Planes compatibles con Microsoft 365

ESET Cloud Office Security es compatible con los siguientes planes de Microsoft 365, Exchange Online y OneDrive.

Planes de Microsoft 365 Enterprise:

- Microsoft 365 Apps for enterprise
- Microsoft 365 E3
- Microsoft 365 E5
- Microsoft 365 F3
- Office 365 E1
- Office 365 E3
- Office 365 E5
- Office 365 F3

Planes de Microsoft 365 Business:

- Microsoft 365 Business Basic
- Microsoft 365 Business Standard
- Microsoft 365 Business Premium
- Microsoft 365 Apps

Planes de Microsoft 365 Education:

- Microsoft 365 A3
- Microsoft 365 A5

Planes de Exchange Online:

- Exchange Online (Plan 1)
- Exchange Online (Plan 2)
- Microsoft 365 Business Standard

Planes de OneDrive:

- OneDrive for Business (Plan 1)
- OneDrive for Business (Plan 2)
- Microsoft 365 Business Basic
- Microsoft 365 Business Standard

Planes de Google Workspace compatibles

ESET Cloud Office Security es compatible con los siguientes planes de Google Workspace.

- Business Starter
- Business Standard
- Business Plus
- Enterprise

Navegadores web compatibles

 Para vivir la mejor experiencia con la consola web de ESET Cloud Office Security, le recomendamos que tenga actualizados los navegadores web.

Puede usar la consola de ESET Cloud Office Security con los siguientes navegadores web:

- Mozilla Firefox 69 y versiones posteriores
- Microsoft Edge 44 y versiones posteriores
- Google Chrome 77 y versiones posteriores
- Opera 63 y versiones posteriores
- Safari 13.x y versiones posteriores

Política de retención de datos y limitaciones

En ciertos casos, existen limitaciones de exploración de ESET Cloud Office Security. No se explorará un archivo y se mostrará en [Registros de la exploración](#) como **No explorado** si ocurre lo siguiente:

- El tamaño del archivo es superior a 200 MB
- La exploración demora más de 2 minutos y se agota el tiempo de la sesión
- El archivo presenta un nivel de anidamiento de 10 o más (por lo general, el archivo se conoce como bomba de archivo o bomba de archivo comprimido)
- El archivo está protegido por contraseña
- El archivo está dañado

Límites de cuarentena (cuando se libera de la cuarentena):

- 15 MB para un archivo adjunto de correo electrónico
- 150 MB para todo el mensaje de correo electrónico, incluidos los archivos adjuntos

Política de retención de datos:

Entidad	Período de retención	Comentario
Objetos en cuarentena	30 días	Se eliminarán de manera permanente los objetos que superen los 30 días.
Detecciones	90 días	Se eliminarán de manera permanente los registros que superen los 90 días.
Registros de la exploración	90 días	Se eliminarán de manera permanente los registros que superen los 90 días.
Registros de la exploración con resultados limpios de exploraciones	3 días	Si tiene una política que utiliza Registrar todos los objetos, los resultados limpios de exploraciones con una antigüedad mayor a 3 días se quitarán de forma permanente.
Copia de seguridad de la base de datos ESET Cloud Office Security	90 días	Se eliminarán de manera permanente las copias de seguridad que superen los 90 días.
Registros de auditoría	90 días	Se eliminarán de manera permanente los registros que superen los 90 días.
Registros de información de la aplicación	90 días	Se eliminarán de manera permanente los registros que superen los 90 días.

Inquilino quitado de la consola ESET Cloud Office Security

Cuando [quita](#) un inquilino de la consola ESET Cloud Office Security, el período de retención de los datos del inquilino es de 30 días (la cuarentena, los registro de la exploración y las estadísticas se eliminarán después de 30 días). Si vuelve a agregar el inquilino en un plazo de 30 días, se restablecerán todos los datos. El resto de los

objetos (inquilinos, usuarios, grupos, sitios, informes, políticas) se quitarán de forma permanente después de 90 días.

ESET Cloud Office Security desactivado en ESET Business Account o ESET MSP Administrator

Si [desactiva](#) ESET Cloud Office Security en ESET Business Account o ESET MSP Administrator, este proceso también quita los inquilinos de ESET Cloud Office Security. La eliminación de ESET Cloud Office Security es permanente y los datos que se eliminan no se pueden restaurar.

Exploración antispam:

ESET Cloud Office Security explora los mensajes de correo electrónico almacenados en casillas de correo en busca de spam. Por este motivo, ESET Cloud Office Security no puede impedir que un usuario envíe un spam a una dirección de correo electrónico externa. En un caso improbable, cuando se roban las credenciales de usuario de Office 365, un spammer puede usar estas credenciales para enviar mensajes de spam masivos (tráfico de correo electrónico saliente).

Licencia para ESET Cloud Office Security

Administre las licencias ESET Cloud Office Security a través de ESET Business Account o ESET MSP Administrator. Pruebe ESET Cloud Office Security con una licencia de [prueba de 30 días](#).

- Consulte [ESET Business Account](#) para crear una cuenta, agregar o administrar una licencia.
- Consulte [ESET MSP Administrator](#) si es un MSP.

ESET Business Account y ESET MSP Administrator (cuenta de licencias híbrida)

Si tiene la misma dirección de correo electrónico registrada en ESET MSP Administrator y ESET Business Account (inicio de sesión único), puede alternar entre las vistas ESET Business Account y ESET MSP Administrator. Proteja a usuarios o empresas que usan [Administración de licencias para ESET Cloud Office Security](#).

Período de gracia para una licencia próxima a vencer de ESET Business Account

Cuando su licencia esté a punto de vencer, se mostrará una alerta en la interfaz de ESET Business Account. Si la fecha de vencimiento pasa, y no ha renovado la licencia o activado una nueva, se mostrará la alerta de vencimiento de la licencia en ESET Business Account. Si no hay una licencia elegible, se mostrará una notificación en ESET Business Account para informar que la licencia se suspenderá en 14 días, y recibirá un correo electrónico a la dirección especificada en su cuenta de administrador.

Tiene un período de gracia de 14 días para renovar después del vencimiento de la licencia. Se le notificará en ESET Business Account y por correo electrónico a la mitad del período de gracia. Después de 14 días, se le suspenderá el uso de ESET Cloud Office Security. No se podrá acceder a la cuenta, la cual dejará de funcionar. Se almacenará una cuenta de ESET Cloud Office Security suspendida, a la que se podrá acceder nuevamente agregando una nueva licencia ESET Cloud Office Security a ESET Business Account. Su cuenta de ESET Cloud Office Security puede permanecer en un estado de suspensión hasta 30 días; luego, se quitará de forma permanente.

Si su cuenta entra en un estado suspendido, se le notificará en ESET Business Account y por correo electrónico cuando falten 14 días para la eliminación de la cuenta. Debe activar una nueva licencia ESET Cloud Office Security para restaurar el acceso a su cuenta ESET Cloud Office Security.

i Los usuarios siguen estando totalmente protegidos durante el período de gracia. Cuando termine el período de gracia, los usuarios dejarán de estar protegidos.

Licencia suspendida

Si no hay una licencia ESET Cloud Office Security válida presente en ESET Business Account, se suspenderá su instancia ESET Cloud Office Security. No se podrá acceder a la instancia, la cual dejará de funcionar. Su instancia de ESET Cloud Office Security puede permanecer en un estado de suspensión hasta 30 días; luego, se quitará de forma permanente. Debe activar una nueva licencia elegible para ESET Cloud Office Security para restaurar el acceso a su instancia de ESET Cloud Office Security.

ESET Business Account

ESET Business Account trabaja como un punto de acceso unificado para ESET Business Account y ESET Cloud Office Security. Use la página de inicio de sesión ESET Cloud Office Security o ESET Business Account para acceder a su ESET Cloud Office Security. Ambas páginas lo redirigen mediante la autenticación de ESET Business Account para verificar su inicio de sesión.

- [Cree una nueva cuenta](#) si no tiene una cuenta registrada en ESET Business Account.
- Si tiene una cuenta de ESET Business Account, [agregue su licencia de ESET Cloud Office Security](#).
- [Administrar](#) ESET Business Account.

Crear una nueva cuenta de ESET Business Account

1. Abra la página de inicio de sesión de [ESET Business Account](#) y haga clic en **Registro gratis**. Complete correctamente el formulario de registro. La dirección de correo electrónico introducida se usará como su nombre de inicio de sesión.
2. La contraseña debe contener, como mínimo, 10 caracteres. Complete su **Nombre** y **Detalles de la compañía** y haga clic en **Continuar**. Lea y confirme que acepta los **Términos de uso de ESET**. Llene el formulario reCAPTCHA y haga clic en **Registrar**.
3. Recibirá un correo electrónico de confirmación después de registrarse correctamente (esto puede demorar hasta 15 minutos). Haga clic en el enlace que se encuentra en el correo electrónico de confirmación para abrir una nueva ventana **Activar cuenta**.
4. Ingrese su contraseña y haga clic en **Activar** para activar su ESET Business Account. Recibirá otro correo electrónico que comprueba que su cuenta de ESET Business Account se creó correctamente. Ahora ya está listo para iniciar sesión en su [ESET Business Account](#).

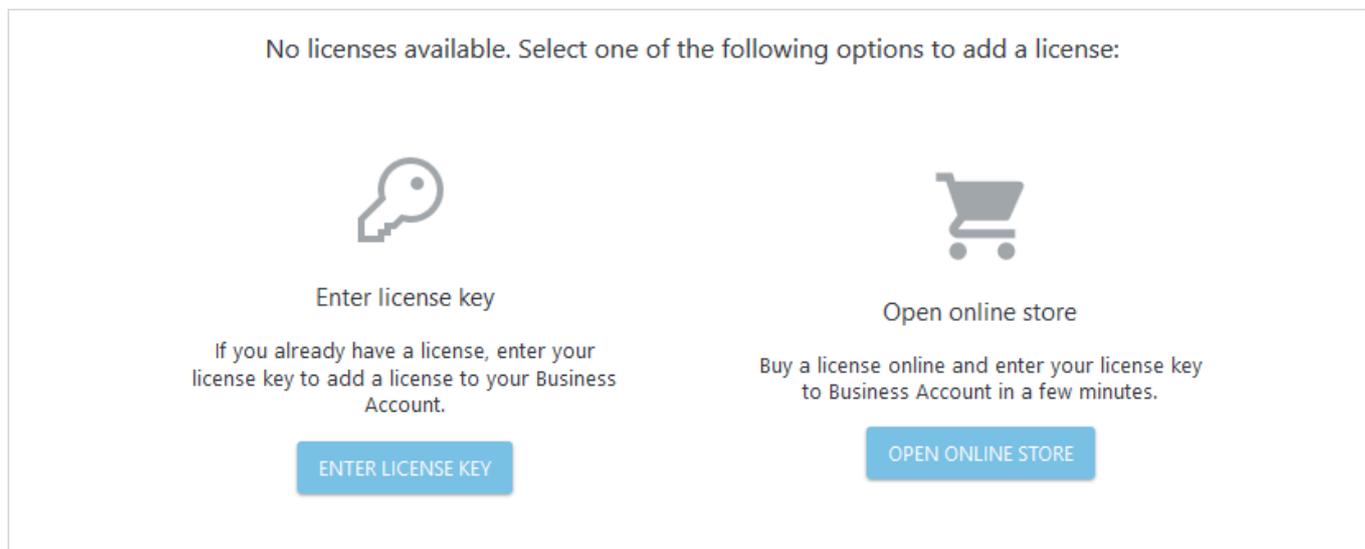
Tras activar ESET Business Account, [agregue su licencia de ESET Cloud Office Security](#).

Agregar licencia de ESET Cloud Office Security en ESET

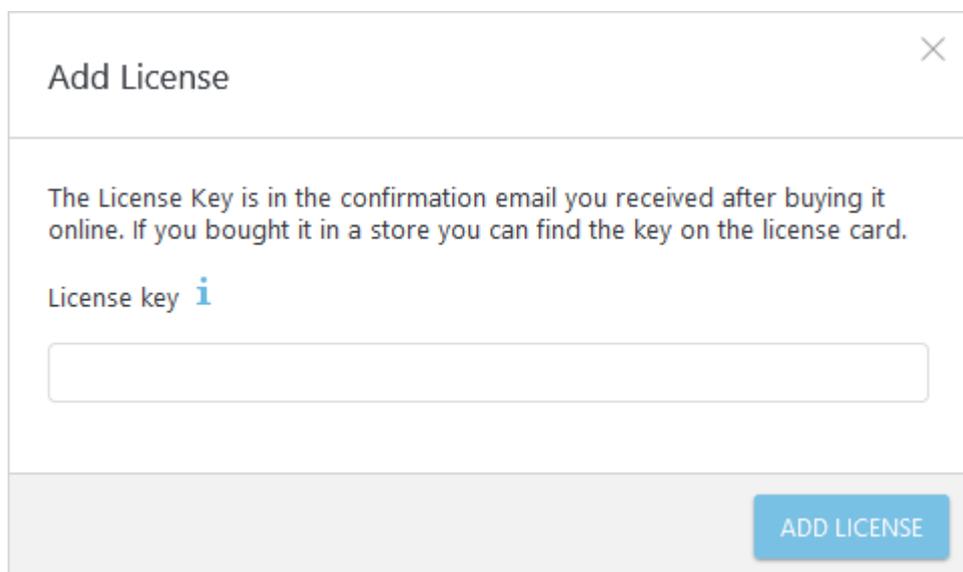
Business Account

Luego de iniciar sesión correctamente en [ESET Business Account](#), verá una pantalla de bienvenida de ESET Business Account si es usuario por primera vez.

1. Haga clic en **Agregar licencia** para abrir la ventana de la licencia. Si es usuario habitual de ESET Business Account, vaya a la pestaña **Licencia** y haga clic en **Agregar licencia**.



2. Introduzca su **clave de licencia** y haga clic en **Agregar licencia**.

A screenshot of the "Add License" dialog box. The title bar says "Add License" with a close button (X) on the right. Below the title bar, there is a paragraph of text: "The License Key is in the confirmation email you received after buying it online. If you bought it in a store you can find the key on the license card." Below this text, there is a label "License key" followed by an information icon (i). Underneath the label is a text input field. At the bottom right of the dialog box, there is a blue button labeled "ADD LICENSE".

3. Recibirá un correo electrónico con un enlace de verificación. Haga clic en el enlace e introduzca sus credenciales de inicio de sesión del portal ESET Business Account cuando se lo soliciten. Para más información sobre la administración de licencias, los usuarios y los sitios, consulte la [guía de ESET Business Account](#).

Administrar ESET Business Account

Actividades habituales relacionadas con las licencias:

Sitios y grupo de licencias

Las licencias y los grupos de licencias se cargan desde ESET Business Account. Los [grupos de licencias](#) están disponibles solo si tiene [sitios](#) existentes en ESET Business Account.

Crear un nuevo usuario en ESET Business Account

Puede crear un usuario para que lo ayude a administrar una parte de sus licencias.

1. Abra [ESET Business Account](#) e inicie sesión.
2. Seleccione **Administración de usuarios**, haga clic en **Nuevo usuario** y escriba la información requerida.
3. Seleccione ESET Cloud Office Security **Derechos de acceso** para un usuario:
 - **Leer**: el usuario tiene acceso a ESET Cloud Office Security y puede ver los usuarios, registros y detecciones, pero no puede administrar políticas, proteger usuarios ni liberar de cuarentena.
 - **Escribir**: el usuario tiene acceso completo a ESET Cloud Office Security y puede ver y administrar usuarios o cuarentenas, o crear políticas
 - **Sin acceso**: el usuario no puede acceder a ESET Cloud Office Security
4. Establezca un idioma en **Preferencias** del usuario para la consola de ESET Cloud Office Security.
5. Haga clic en **Crear** y se creará el usuario.

Crear un nuevo sitio en ESET Business Account

Los sitios le permiten dividir o combinar sus licencias en grupos de licencias. Los sitios son grupos individuales que pueden tener su propia ubicación y sus propios administradores.

1. Abra [ESET Business Account](#) e inicie sesión.
2. Seleccione **Detalles**, haga clic en **Crear sitio** y escriba la información personal requerida.
3. Haga clic en **Agregar usuario**, seleccione un usuario y haga clic en **Confirmar**.
4. En el grupo de licencias, haga clic en **Agregar unidades** y seleccione una licencia para ESET Cloud Office Security. Puede modificar las **subunidades** y hacer clic en **Confirmar**.
5. Haga clic en **Crear** y se creará el sitio.

ESET MSP Administrator

ESET MSP Administrator es un sistema de administración de licencias que permite a los usuarios de proveedor de servicios gestionados crear varios clientes de proveedor de servicios gestionados y generar licencias específicas con conteo de puestos. El portal de licencias de ESET MSP Administrator admite precios por volumen y facturación en función de un número exacto de días de puesto adquiridos.

ESET Cloud Office Security está disponible tanto para MSP Managers como para MSPs y managed MSPs. El usuario ESET MSP Administrator con acceso de escritura es elegible para activar ESET Cloud Office Security. Los usuarios pueden acceder a ESET Cloud Office Security mediante derechos de acceso de Escritura, Lectura o Personalizados.

- [Cree un nuevo Cliente MSP](#) (se requiere la dirección de correo electrónico del cliente para la activación de la consola ESET Cloud Office Security).
- [Activar](#) ESET Cloud Office Security desde ESET MSP Administrator.

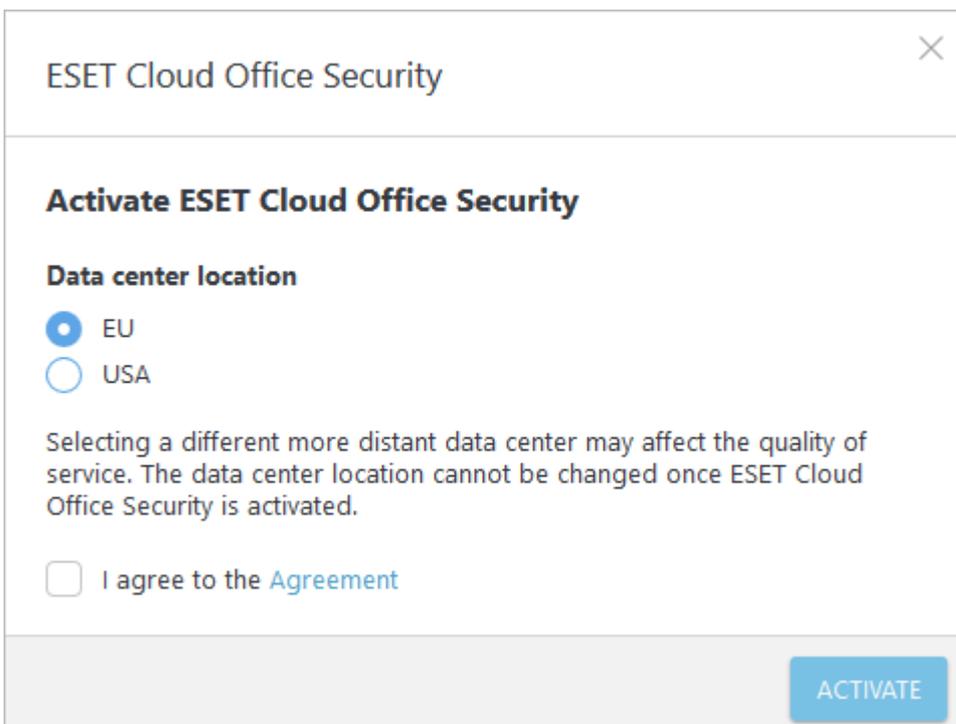
Activar ESET Cloud Office Security

1. Inicie sesión en [ESET Business Account](#) o [ESET MSP Administrator](#) y ubique el ESET Cloud Office Security mosaico en el **Dashboard**.
2. Haga clic en **Activar** en el extremo inferior derecho del mosaico ESET Cloud Office Security.



3. El asistente de activación hará referencia a los [Términos de uso](#) de ESET Cloud Office Security y mostrará la ubicación óptima del centro de datos según su ubicación actual. Seleccione **Acepto los Términos de uso** y haga clic en **Activar**. No recomendamos cambiar la ubicación del centro de datos; sin embargo, puede realizar la selección si necesita usar otra ubicación.

i Los centros de datos son totalmente independientes. Una vez que selecciona la ubicación del centro de datos, no puede modificarse y no puede migrar a otra ubicación. Para cambiar el centro de datos, inicie el proceso de activación desde el comienzo.

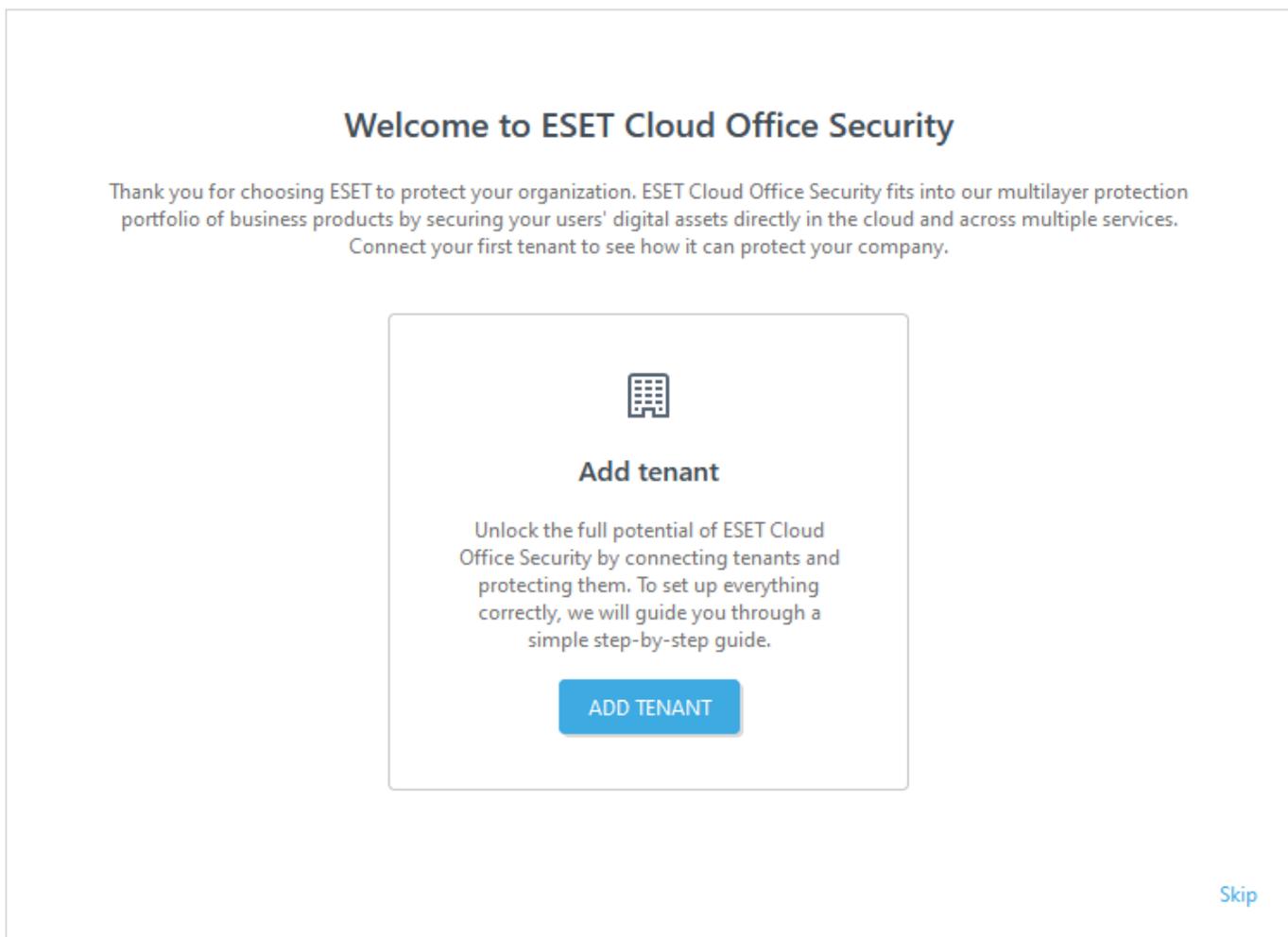


4. Haga clic en **Abrir** en el mosaico ESET Cloud Office Security. Se abrirá el [Dashboard](#) de ESET Cloud Office Security en una nueva pestaña del navegador.

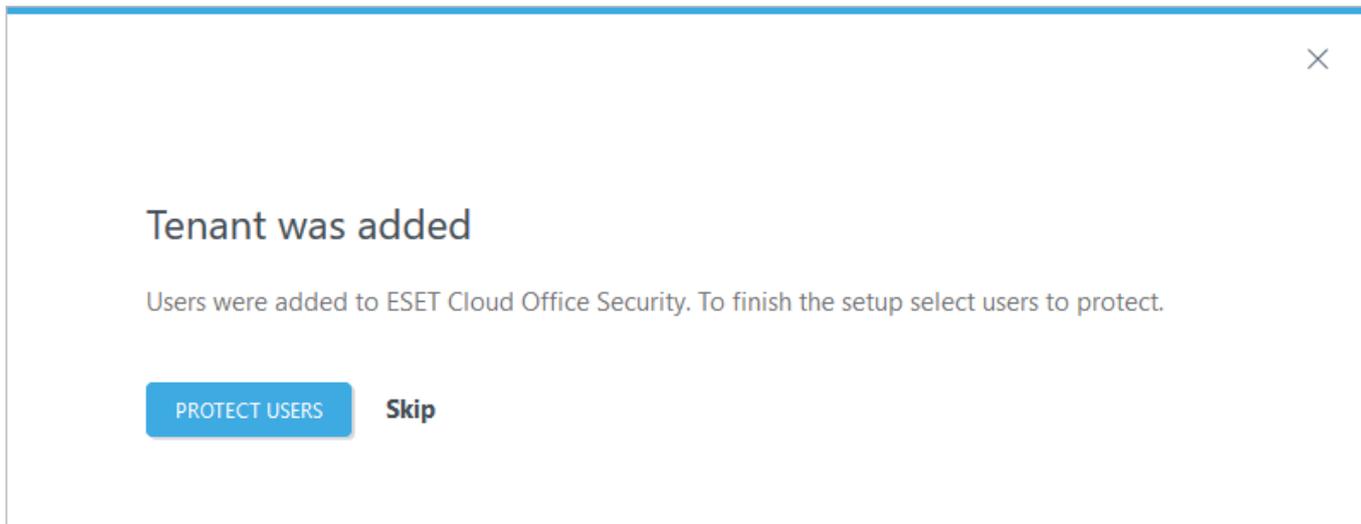


Al iniciar sesión en ESET Cloud Office Security por primera vez, aparecerá un **asistente de inicio**. Este asistente lo guía por el proceso de instalación inicial.

1. [Añada su inquilino](#) ([Microsoft 365](#) o [Google Workspace](#)).

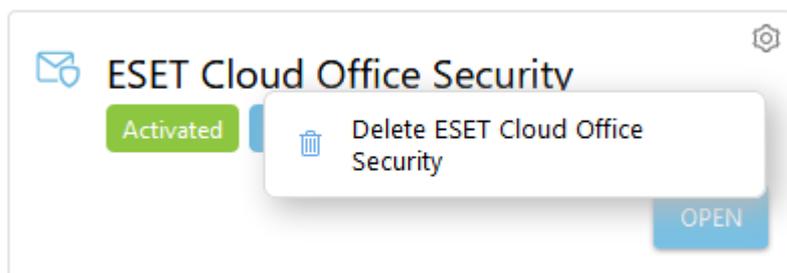


2. [Proteger a los usuarios](#). Si presiona **Omitir**, más adelante podrá proteger al usuario o las empresas mediante [Gestión de licencias para ESET Cloud Office Security](#).

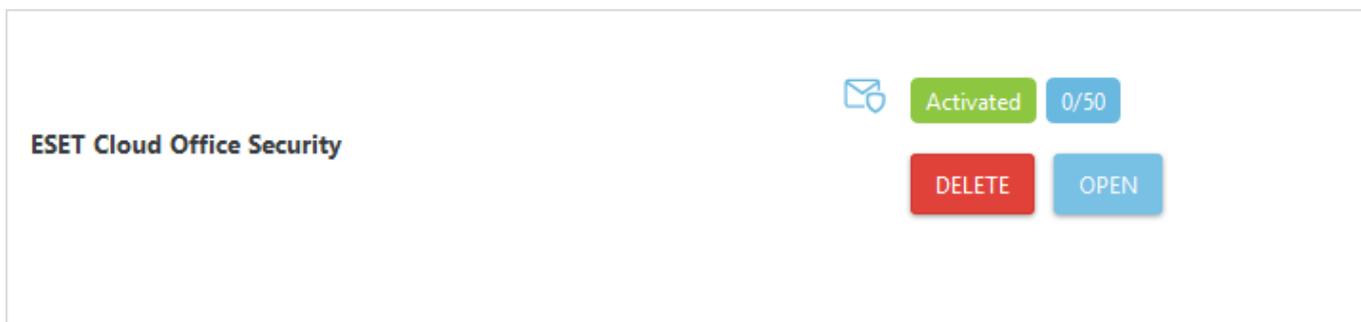


Desactivar ESET Cloud Office Security

1. Inicie sesión en [ESET Business Account](#) o [ESET MSP Administrator](#) y ubique el ESET Cloud Office Security mosaico en el **Dashboard**.
2. Haga clic en el ícono de engranaje  que se encuentra en el extremo superior derecho de ESET Cloud Office Security y seleccione **Quitar ESET Cloud Office Security**.



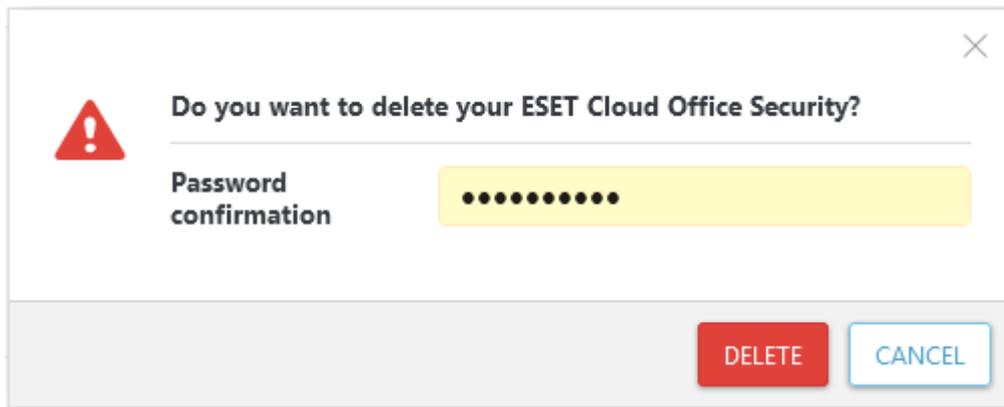
3. De manera alternativa, vaya a la sección **Detalles** y haga clic en **Eliminar**.



4. Se abre una ventana de advertencia que le avisa que se eliminarán todos los datos. Ingrese su contraseña de ESET Business Account para confirmar y haga clic en **Eliminar**.



ESET Cloud Office Security se quitará de forma permanente. Los datos que se quitaron no se podrán restaurar.



Se ha eliminado la instancia de ESET Cloud Office Security y el mosaico de producto de ESET Cloud Office Security se revierte al estado **No activado**. También recibirá un correo electrónico de confirmación de ESET Business Account.

Administrar los inquilinos en Configuración

Administrar inquilinos conectados a ESET Cloud Office Security. Puede ver todos los inquilinos registrados en la tabla con detalles para cada inquilino. Utilice el botón Actualizar para volver a cargar la tabla con inquilinos.

Si desea agregar un nuevo inquilino, haga clic en [Agregar inquilino](#) y elija [Microsoft 365](#) o [Google Workspace](#) según la plataforma en la nube que desee proteger. Una vez finalizado el proceso de registro de inquilinos, Microsoft 365 o Google Workspace estará protegido por ESET Cloud Office Security.

Después de agregar el inquilino, la pantalla cambia, mostrando la lista de inquilinos asociados con un sitio, puede administrar su inquilino existente o agregar más inquilinos. La tabla muestra el nombre del inquilino, el número de usuarios, cuándo se agregó el inquilino, la configuración de idioma, los usuarios con licencia de Microsoft 365, el nombre del sitio y el administrador de Google.

The screenshot shows the ESET Cloud Office Security interface. The top navigation bar includes the ESET logo, "CLOUD OFFICE SECURITY", and user information for VIKTOR VINCZLÉR. The main content area is titled "Settings" and "Tenants". Below the title, there is a table of tenants with columns for Tenant, Users, Added, Language, Microsoft 365 Lic..., Site, and Google Admin. Two tenants are listed: one with 16 users and one with 11 users. Below the table are buttons for "ADD TENANT", "REMOVE", and a refresh icon.

TENANT	USERS	ADDED	LANGUAGE	MICROSOFT 365 LIC...	SITE	GOOGLE ADMIN
<input type="checkbox"/> G...	16	01/08/2023 15:02	English	N/A	Eset	admin@...
<input type="checkbox"/> M...	11	01/08/2023 15:04	English	<input type="checkbox"/>	Eset	N/A

Idioma

Este ajuste determina el idioma de los mensajes de notificación de correo electrónico a los miembros del inquilino. Puede definir el idioma de cada inquilino por separado; por ejemplo, en el caso de MSP que administra varias empresas.

Para eliminar un inquilino de ESET Cloud Office Security, seleccione el inquilino correspondiente y haga clic en [Eliminar](#). Se mostrará una ventana de confirmación para que pueda tomar la decisión final. Una vez eliminados, los datos de usuario se eliminarán luego de 30 días.

Usuarios con licencia de Microsoft 365

Esta opción está activada de forma predeterminada. Equivale a una lista de usuarios del [Centro de administración de Microsoft 365](#) en **Usuarios > usuarios Activos > Filtro: Usuarios con licencia**.

Si se deshabilita esta opción, ESET Cloud Office Security mostrará todos los usuarios, incluidos los usuarios sin una licencia de Microsoft 365 (por ejemplo, buzones de correo compartidos). Si utiliza la protección automática para un grupo o inquilino que contiene usuarios sin licencia de Microsoft 365, estos usuarios se tornarán visibles, estarán protegidos y consumirán unidades de licencia de ESET Cloud Office Security. El estado de protección de los usuarios recientemente visibles podrá quedar como **Pendiente** hasta por una hora. Una vez finalizado el proceso de protección automática, el estado de protección cambiará a **Protegido** u otros posibles [estados](#) en la sección Usuarios.

i Si su inquilino o grupo con protección automática contiene un usuario sin buzón de correo ni OneDrive, este usuario consumirá una unidad de licencia de ESET Cloud Office Security. Verá el [estado de protección Advertencia](#) para este usuario.

Si se vuelve a habilitar la opción Usuarios con licencia de Microsoft 365, solo se mostrarán los usuarios que tienen licencia de Microsoft 365. Si tenía usuarios con protección automática sin licencia de Microsoft 365, desaparecerán de la sección Usuarios y se liberarán unidades de licencia ESET Cloud Office Security. El cambio puede demorar hasta 1 hora en aplicarse.

i Si protegió de forma manual a los usuarios sin licencia de Microsoft 365 (mientras la configuración **Usuarios con licencia de Microsoft 365** estaba habilitada), estos usuarios seguirán estando visibles y protegidos, incluso, luego de habilitar la opción **Usuarios con licencia de Microsoft 365** (hasta que se desproteja a los usuarios).

Sitio

Si desea cambiar el sitio al que está asociado el inquilino, haga clic en el nombre del sitio para abrir la ventana **Seleccionar un sitio para proteger** y realice los cambios necesarios.

Administrador de Google

El administrador de Google debe ser un correo electrónico activo de su administrador de Google Workspace.

! Si la función o la dirección de correo electrónico del administrador están a punto de cambiar, actualice la información de administrador de Google haciendo clic en ella. Haga esto por adelantado para garantizar la funcionalidad del inquilino y la protección de su sitio.

Actualizar consentimiento

Si se muestra un botón amarillo, puede actualizar su consentimiento. La actualización del consentimiento para el inquilino existente extiende los permisos de ESET Cloud Office Security a su cuenta de Microsoft 365, lo que habilita una característica que proporciona información sobre el tipo de usuario. El tipo de usuario se define en Azure Active Directory y se mostrará en la sección [Usuarios](#) en una columna dedicada. Por ejemplo, puede filtrar los usuarios de Microsoft 365 en función de su tipo si solo desea enumerar los buzones compartidos.

Haga clic en el botón **Actualizar** para cada inquilino para el que desee habilitar esta característica. La actualización del tipo de usuario de Azure AD puede tardar hasta 24 horas.

Si se muestra un botón rojo, significa que se ha revocado el consentimiento o que se ha realizado otro cambio que afectó la integración del inquilino con ESET Cloud Office Security. Haga clic en el botón **Actualizar** si desea seguir protegiendo a los usuarios.

Agregar su primer inquilino

Para proteger la plataforma en la nube, haga clic en **Agregar inquilino** para conectar Microsoft 365 o Google Workspace a ESET Cloud Office Security.

Welcome to ESET Cloud Office Security

Thank you for choosing ESET to protect your organization. ESET Cloud Office Security fits into our multilayer protection portfolio of business products by securing your users' digital assets directly in the cloud and across multiple services. Connect your first tenant to see how it can protect your company.



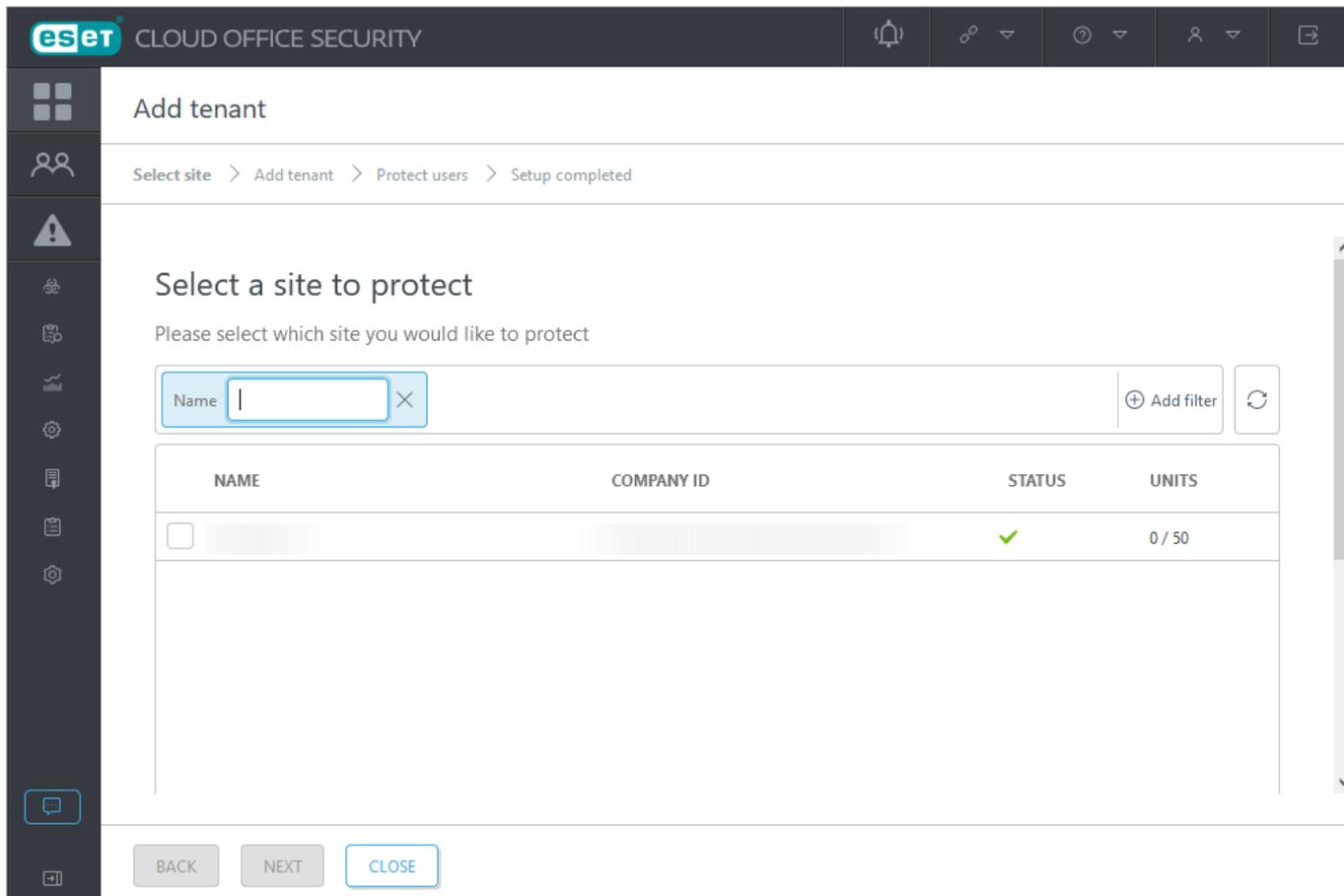
Add tenant

Unlock the full potential of ESET Cloud Office Security by connecting tenants and protecting them. To set up everything correctly, we will guide you through a simple step-by-step guide.

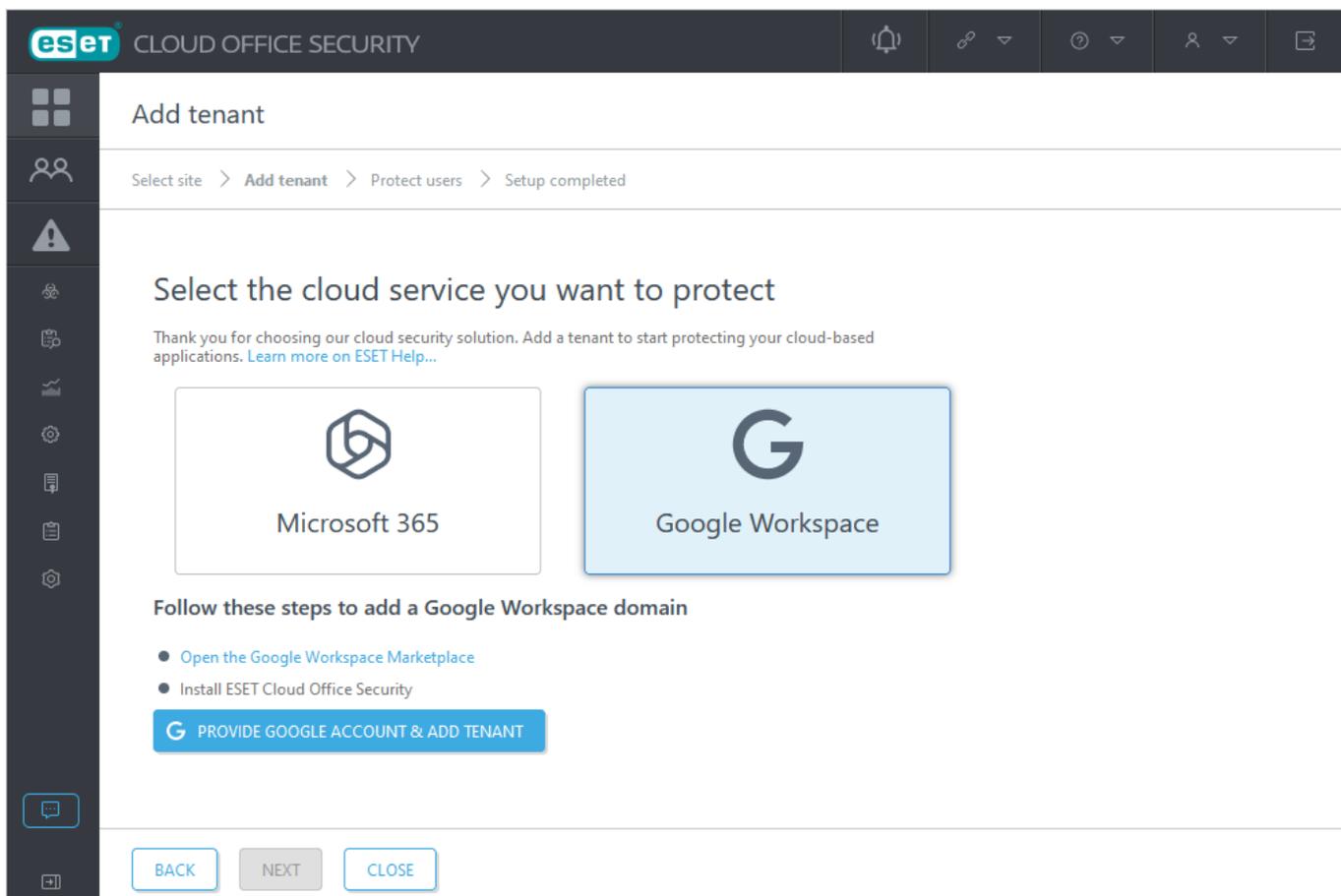
ADD TENANT

[Skip](#)

Debería ver una lista de sitios disponibles en la ventana **Seleccionar un sitio para proteger**. Use la casilla de verificación para seleccionar el sitio que desea asociar a un inquilino y haga clic en **Siguiente**.



Haga clic en el mosaico de [Microsoft 365](#) o [Google Workspace](#) en la ventana **Seleccionar el servicio en la nube que desea proteger** y siga los pasos de las viñetas:



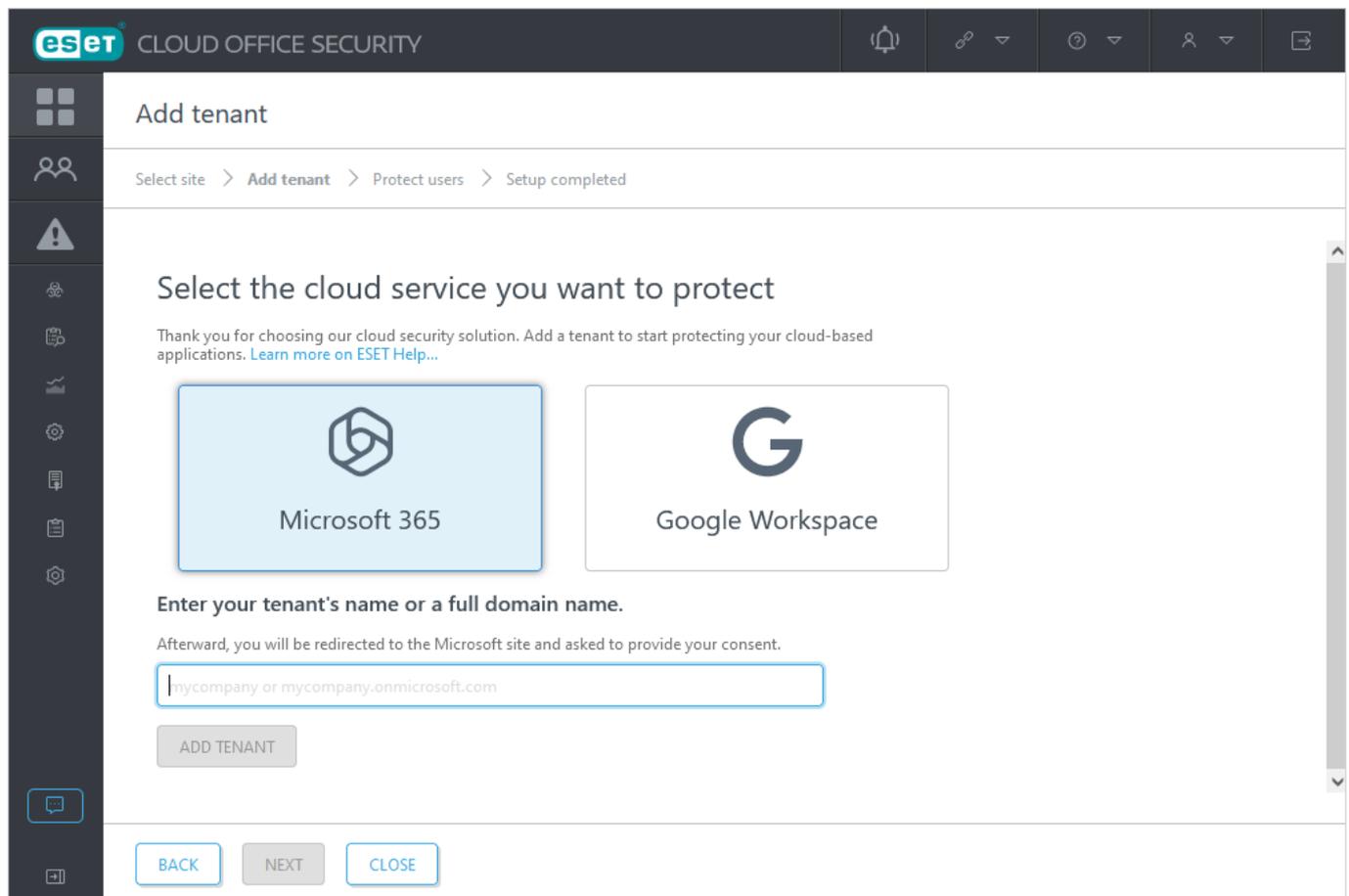
Inquilino de Microsoft 365

Azure Active Directory (Azure AD) organiza los objetos, como usuarios y aplicaciones, en grupos llamados inquilinos. Una manera habitual de identificar a un inquilino es por el nombre de dominio. Si varios usuarios comparten un nombre de dominio, estos usuarios forman parte del mismo inquilino. Los inquilinos le permiten definir políticas sobre los usuarios y aplicaciones de su organización para cumplir con las políticas de seguridad y operativas. Puede proteger y administrar múltiples inquilinos de Microsoft 365 desde una sola consola de ESET Cloud Office Security.

Para más información, consulte el artículo de Microsoft sobre [Inquilinos en Azure Active Directory](#).

Agregar inquilino

1. Vaya a **Configuración** y haga clic en **Agregar inquilino** (o en cualquier lugar donde vea el botón **Agregar inquilino**).
2. Haga clic en el mosaico de **Microsoft 365**.



The screenshot shows the ESET Cloud Office Security interface. The top navigation bar includes the ESET logo and 'CLOUD OFFICE SECURITY'. The main content area is titled 'Add tenant' and shows a breadcrumb trail: 'Select site > Add tenant > Protect users > Setup completed'. The primary instruction is 'Select the cloud service you want to protect'. Two tiles are presented: 'Microsoft 365' (highlighted with a blue border) and 'Google Workspace'. Below these, a text box prompts the user to 'Enter your tenant's name or a full domain name.' with a note that they will be redirected to the Microsoft site for consent. The input field contains the placeholder 'mycompany or mycompany.onmicrosoft.com'. An 'ADD TENANT' button is positioned below the input field. At the bottom of the interface, there are three buttons: 'BACK', 'NEXT', and 'CLOSE'.

3. Escriba su nombre de inquilino de Microsoft 365 o su nombre de dominio completo y haga clic en **Agregar inquilino**.
4. Se lo direccionará a la página de consentimiento de Microsoft Online con una lista de permisos requerida por ESET Cloud Office Security.

Add tenant

Select site > **Add tenant** > Protect users > Setup completed

Select the cloud service you want to protect

Thank you for choosing our cloud security solution. Add a tenant to start protecting your cloud-based applications. [Learn more on ESET Help...](#)

Organization: esethqsupport.onmicrosoft.com

Redirecting to Microsoft site...

5. Ingrese sus credenciales de cuenta de administrador de Microsoft 365 para permitir el ESET Cloud Office Security acceso a datos ubicados en su cuenta de Microsoft; haga clic en **Aceptar**.



.onmicrosoft.com

Permissions requested Review for your organization

ESET Cloud Office Security

This application is not published by Microsoft or your organization.

This app would like to:

- ✓ Read and write all applications
- ✓ Read directory data
- ✓ Read and write files in all site collections
- ✓ Read all groups
- ✓ Read and write mail in all mailboxes
- ✓ Read all hidden memberships
- ✓ Create, edit, and delete items and lists in all site collections
- ✓ Read all users' full profiles
- ✓ Sign in and read user profile
- ✓ Read and write items and lists in all site collections

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

Accept

6. Se agregó el inquilino de Microsoft 365, incluidos los usuarios.

Add tenant

Select site > **Add tenant** > Protect users > Setup completed



Tenant was added

Users were added to ESET Cloud Office Security. To finish the setup select users to protect.

7. Para finalizar la configuración, haga clic en **Siguiente** y seleccione los usuarios que desee **Proteger**.

Add tenant

Select site > Add tenant > Protect users > **Setup completed**



You're all set

Tenant **example.com** added to ESET Cloud Office Security

ADD ANOTHER TENANT

Inquilino de Google Workspace

Integre su inquilino de Google Workspace con ESET Cloud Office Security para habilitar la protección de los usuarios de Google Workspace.

Agregar inquilino

1. Vaya a **Settings (Configuración)** y haga clic en **Add tenant (Agregar inquilino)** (o en cualquier lugar donde vea el botón **Add tenant (Agregar inquilino)**).

2. Haz clic en el mosaico de **Google Workspace**.

The screenshot shows the ESET Cloud Office Security interface. At the top, the header reads "eset CLOUD OFFICE SECURITY". Below the header, there is a navigation bar with "Add tenant" selected. A breadcrumb trail shows "Select site > Add tenant > Protect users > Setup completed". The main content area is titled "Select the cloud service you want to protect" and includes a thank-you message. Two cards are displayed: "Microsoft 365" and "Google Workspace". The "Google Workspace" card is highlighted with a blue border. Below the cards, the text "Follow these steps to add a Google Workspace domain" is followed by a list of steps: "Open the Google Workspace Marketplace" and "Install ESET Cloud Office Security". A prominent blue button with a white 'G' icon and the text "PROVIDE GOOGLE ACCOUNT & ADD TENANT" is positioned below the list. At the bottom of the interface, there are three buttons: "BACK", "NEXT", and "CLOSE".

3. Haga clic en [Open the Google Workspace Marketplace \(Abrir Google Workspace Marketplace\)](#) e instale la ESET Cloud Office Security aplicación con una cuenta de administrador. Actualmente, la aplicación [ESET Cloud Office Security](#) solo está disponible en Google Workspace Marketplace a través del enlace directo de este asistente.

Google Workspace Marketplace

Search apps

Sign in

ESET Cloud Office Se...

Admin install

Individual install

ESET Cloud Office Security provides advanced protection for Google Workspace and Microsoft 365 apps, with ultimate zero-day threat defense.

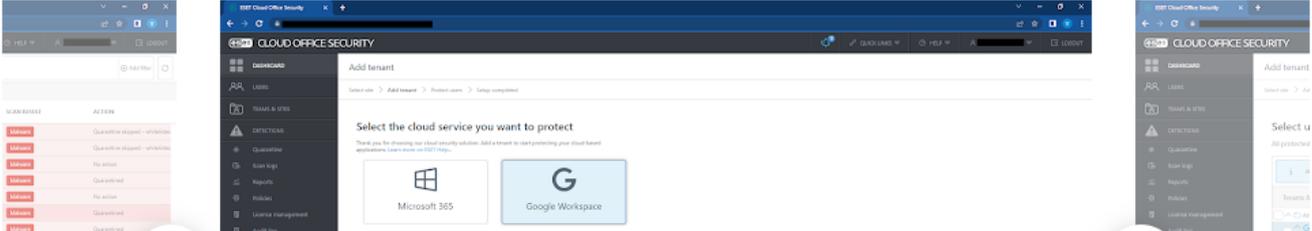
By: [ESET](#)

Listing updated: July 24, 2023

⚠️ This application requires administrator privileges to be installed. [Learn more](#)

No reviews ⓘ ↓ 14

Overview Permissions Reviews



4. Haga clic en **Continue (Continuar)** en la pantalla **Admin install (Instalación de administrador)**.

Admin install

You are about to install this app for an entire Google Workspace organization, or for specific organizational units or groups. All users of the Google Workspace organization, organizational units, or groups you select will have access to this app.

It may take up to 24 hours for this app to be installed for your entire Google Workspace domain, organizational units, or groups.

ESET Cloud Office Security needs your permission in order to start installing.

By clicking Continue, you acknowledge that your information will be used in accordance with the [terms of service](#) and [privacy policy](#) of this application.

CANCEL **CONTINUE**

5. Asegúrese de que la opción **Everyone at your organization (Todos en su organización)** esté seleccionada en la pantalla de derechos de acceso. Además, la casilla Términos de servicio y Política de privacidad debe estar activada antes de hacer clic en **Finish (Finalizar)**.



You are granting **ESET Cloud Office Security** the right to access your data:

-  See, edit, create, and delete all of your Google Drive files 
-  Read, compose, send, and permanently delete all your email from Gmail 
-  View customer related information 
-  View domains related to your customers 
-  View groups on your domain 
-  View organization units on your domain 
-  See info about users on your domain 
-  See your primary Google Account email address 
-  See your personal info, including any personal info you've made publicly available 

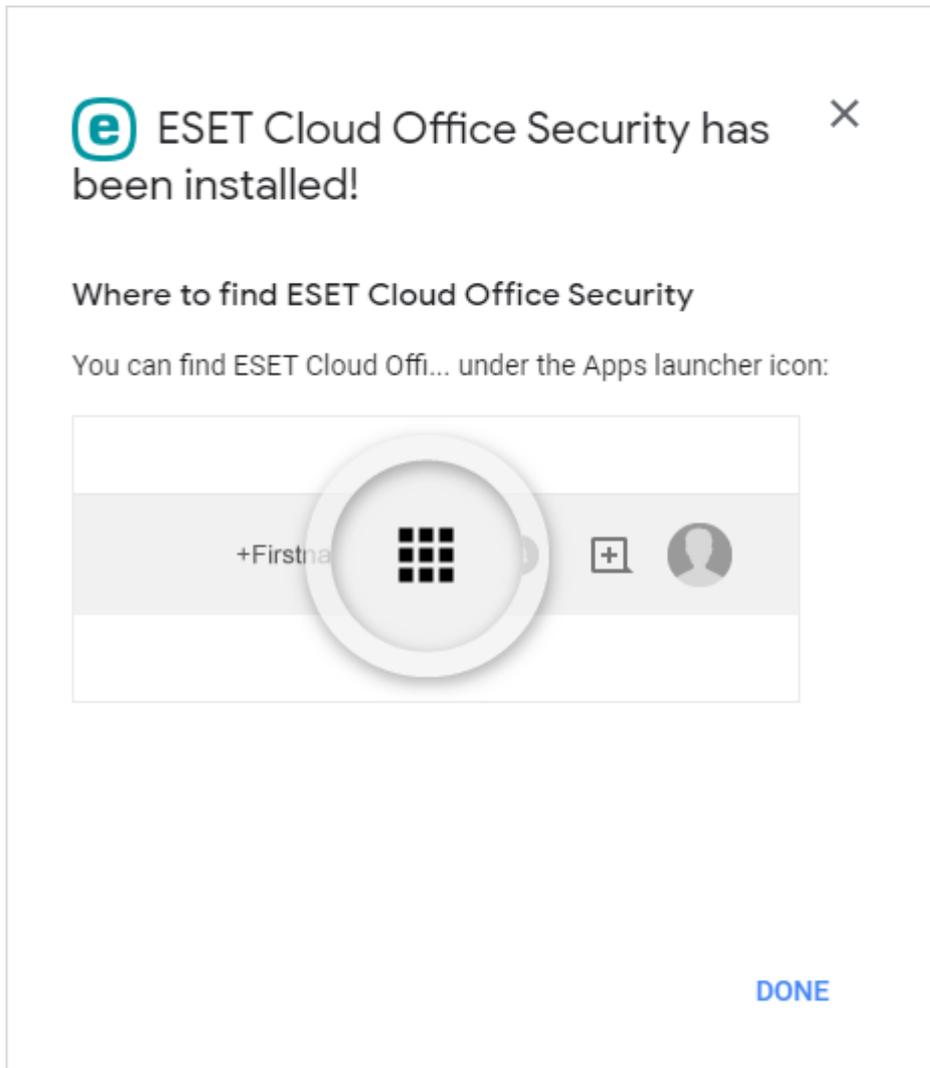
Install the app automatically for the following users

- Everyone at your organization
- Certain groups or organizational units
Select users in the next step
- I agree to the application's [Terms of Service](#), [Privacy Policy](#), and Google Workspace Marketplace's [Terms of Service](#)

CANCEL

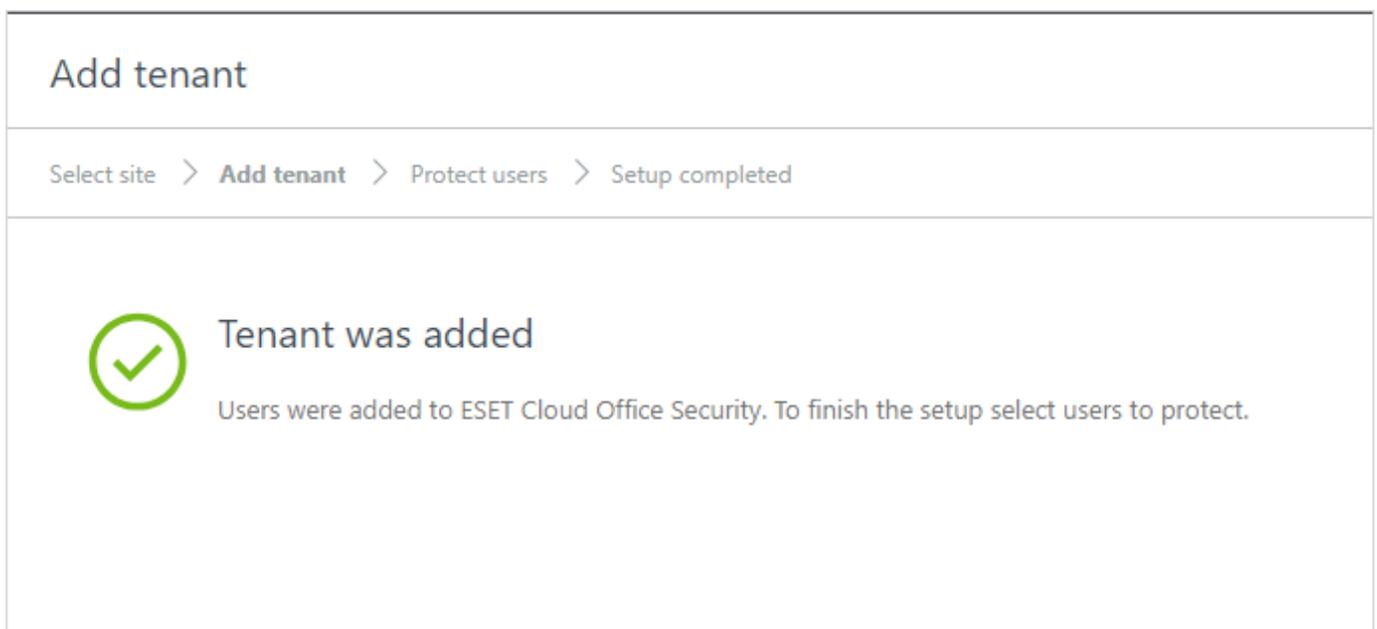
FINISH

6. La aplicación ESET Cloud Office Security está instalada, haga clic en **Done (Listo)**.

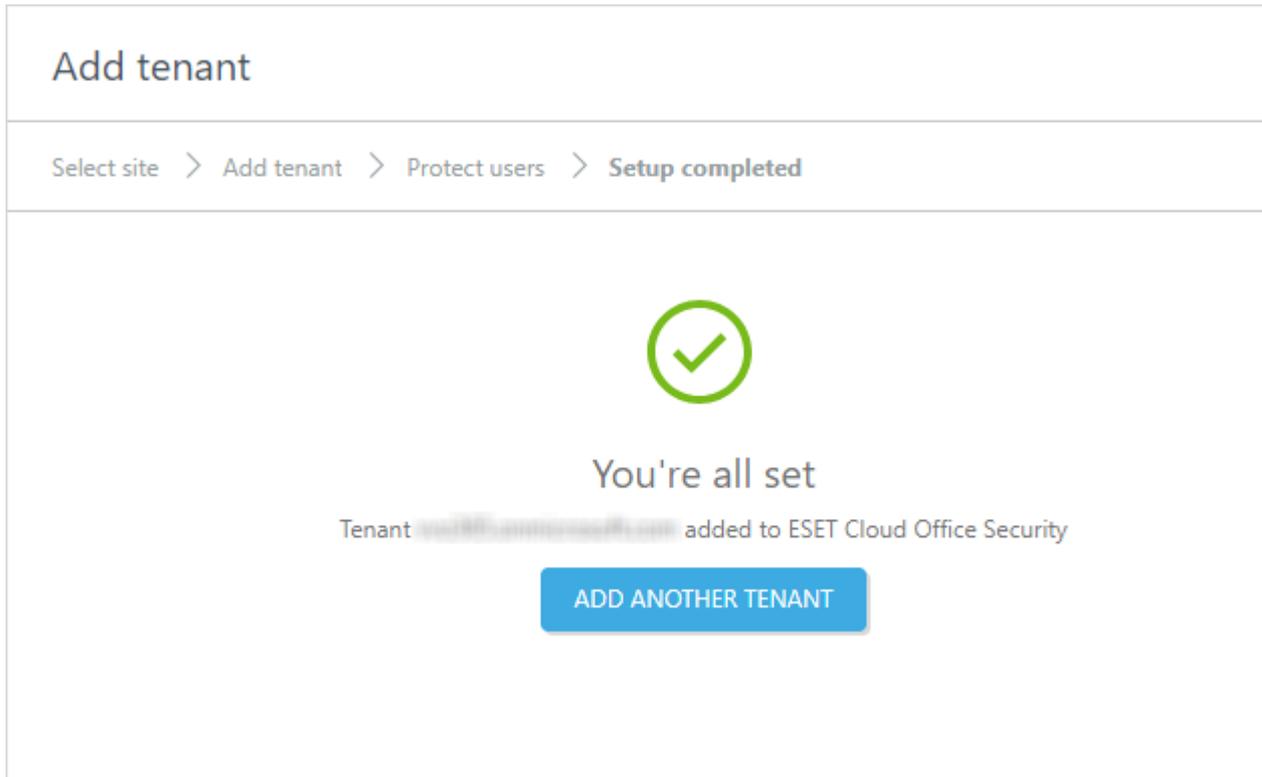


7. Una vez que se completa la aplicación ESET Cloud Office Security, vuelva a la consola de ESET Cloud Office Security. Haga clic en **Proporcionar una cuenta y agregar inquilino** para verificar la propiedad y continuar.

8. Se ha añadido su inquilino de Google Workspace, incluidos los usuarios.

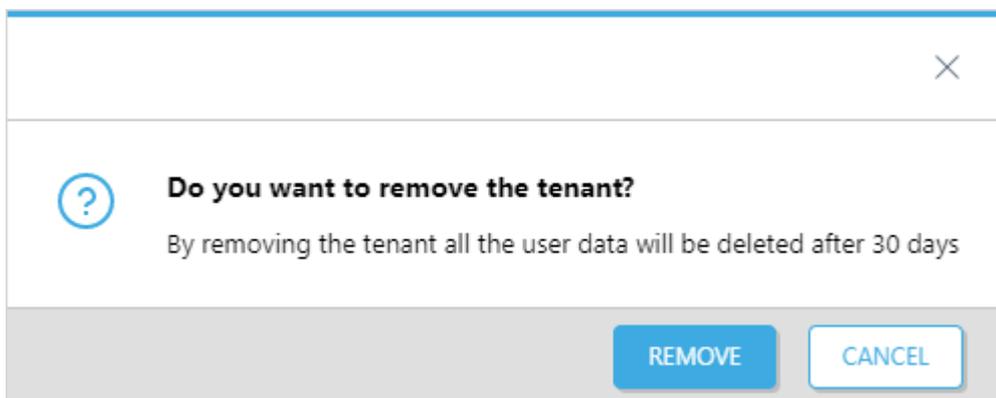


9. Para finalizar la configuración, haga clic en **Siguiente** y seleccione los usuarios que desee **Proteger**. Está todo listo.



Quitar inquilino de ESET Cloud Office Security

1. Seleccione **Configuración**.
2. Seleccione el inquilino correspondiente y haga clic en **Eliminar**.
3. En una ventana de notificación se advierte que este proceso quitará los datos tal como se describe en la [Política de retención de datos y limitaciones](#), y los usuarios perderán la protección. Haga clic en **Quitar** para confirmar la eliminación.



i Cuando quita un inquilino de la consola de ESET Cloud Office Security, el período de retención de los datos del inquilino es de 30 días (la cuarentena, los registros de la exploración y las estadísticas se eliminan después de 30 días). Si vuelve a agregar el inquilino en un plazo de 30 días, se restablecerán todos los datos. El resto de los objetos (inquilinos, usuarios, grupos, sitios, informes, políticas) se quitarán de forma permanente después de 90 días. Para obtener más información, consulte la [Política de limitaciones y retención de datos](#).

Eliminar ESET Cloud Office Security del portal de Azure

1. Inicie sesión en el [portal de Azure](#) con una cuenta de administrador.

! Para eliminar una aplicación, debe ser el propietario de la aplicación o tener privilegios de administrador.

2. Vaya al servicio de **Azure Active Directory** y seleccione **Aplicaciones empresariales**.

3. Busque y haga clic en la aplicación **ESET Cloud Office Security** en la página de descripción general, vaya a **Propiedades** y haga clic en **Eliminar**.

Navegue por el ESET Cloud Office Security

Mire cómo navegar a través de la interfaz de ESET Cloud Office Security. Pronto podrá familiarizarse con los elementos y herramientas de navegación de ESET Cloud Office Security, que pretenden ser intuitivos y fáciles además de ser interactivos.

Use la barra de navegación ubicada a la izquierda para alternar entre distintas partes de la consola de ESET Cloud Office Security:

 [Usuarios](#)

 [Equipos y sitios](#)

 [Detecciones](#)

 [Cuarentena](#)

 [Registros de la exploración](#)

 [Informes](#)

 [Políticas](#)

 [Administración de licencias](#)

 [Registro de auditoría](#)

 [Configuración](#)

 **Contraer:** ampliar y contraer el menú de navegación. Al contraer el panel, se deja más espacio libre de

pantalla en el Dashboard. Haga clic en el ícono  para expandir el panel de navegación.

La barra de herramientas en la parte superior está disponible en todo momento:



 **Navegador de productos:** acceso rápido a las consolas de ESET y otros enlaces útiles. (Puede ver los productos respectivos en función de su licencia y derechos de acceso).

 **ESET Business Account y ESET MSP Administrator** (cuenta de licencias híbridas): si tiene la misma dirección de correo electrónico registrada en ESET MSP Administrator y ESET Business Account (inicio de sesión único), puede alternar entre las vistas ESET Business Account y ESET MSP Administrator.

 **Mostrar notificaciones:** para ver todas las notificaciones, haga clic en el ícono de la campana , ubicado en la barra superior.

 **Vínculos rápidos:** permite acceder fácilmente a Agregar inquilino, Nueva política, ESET Business Account o ESET MSP Administrator.

 **Ayuda:** el primer enlace de este menú siempre vincula a la ayuda en línea de la pantalla actual. Si no puede resolver un problema, busque la [Base de conocimiento de ESET](#) o el [foro de soporte](#). También puede [Enviar comentarios](#) o **Enviar una muestra para su análisis**. Abra la página Acerca de en la que se proporciona información detallada sobre la versión ESET Cloud Office Security y se establece un enlace a los documentos legales.

 **Usuario** (que ha iniciado sesión) – Muestra el nombre de usuario. Haga clic en **Establecer tema** y seleccione el deseado en el menú desplegable:

- **Tema predeterminado (claro):** ESET Cloud Office Security usará un esquema de color claro (estándar).
- **Tema oscuro:** ESET Cloud Office Security usará un esquema de colores oscuros (modo oscuro).
- **Tema del sistema operativo:** la combinación de colores de ESET Cloud Office Security se basa en la configuración del sistema operativo.

 **Salir de sesión:** presione este pictograma siempre presente para salir de la consola ESET Cloud Office Security.

Cambiar idioma del portal de ESET Cloud Office Security

Inicie sesión en [ESET Business Account](#) o [ESET MSP Administrator](#), vaya a **Administración de usuarios** y **Editar** usuario. Busque la configuración del idioma de ESET Cloud Office Security, cambie al idioma de preferencia y haga clic en **Guardar** antes de abandonar la pantalla **Perfil**.

Profile

PREFERENCES

Language

ESET BUSINESS ACCOUNT

ESET CLOUD OFFICE SECURITY

English

English

Time zone

(UTC+01:00) Amsterdam, Berlin, Bern, Rom

ESET LiveGuard Advanced

ESET LiveGuard Advanced provee otra capa de seguridad mediante el uso de la tecnología basada en la nube avanzada de ESET para detectar nuevos tipos de amenazas nunca antes vistos. ESET LiveGuard Advanced le da la ventaja de estar protegido contra posibles consecuencias provocadas por nuevas amenazas. Si ESET LiveGuard Advanced detecta un código o comportamiento sospechoso, evita mayor actividad de amenazas al colocarlo temporalmente en cuarentena.

Una muestra sospechosa (archivo o mensaje de correo electrónico) se envía automáticamente a ESET Cloud, donde el servidor de ESET LiveGuard Advanced la analiza con motores de detección de malware de vanguardia. Mientras los archivos o los correos electrónicos se encuentran en cuarentena, ESET Cloud Office Security espera los resultados del servidor de ESET LiveGuard Advanced.

Después de completar el análisis, ESET Cloud Office Security recibe un informe con un resumen del comportamiento de la muestra observada. Si la muestra resulta inofensiva, se libera de la cuarentena. De lo contrario, se mantiene en cuarentena.

Los resultados de ESET LiveGuard Advanced para las muestras suelen llegar en cuestión de minutos para los mensajes de correo electrónico. Sin embargo, el intervalo de espera predeterminado es de 5 minutos. En casos raros, cuando los resultados de ESET LiveGuard Advanced no llegan dentro del intervalo, el mensaje se libera. Puede cambiar el intervalo a su tiempo preferido (cualquier opción entre 5 y 60 minutos, en incrementos de un minuto).

La licencia ESET Cloud Office Security le permite usar la función ESET LiveGuard Advanced sin tarifas adicionales. Verá la etiqueta ELG junto al ID de la licencia en [Administración de licencias](#).

Cuando aparezca una ventana emergente pequeña, podrá activar ESET LiveGuard Advanced mediante la creación de una [política](#) nueva o la actualización de una existente.

Enable ESET LiveGuard by creating or updating an existing policy

DISMISS

CREATE NEW POLICY

Para obtener información más detallada sobre ESET LiveGuard Advanced, consulte [Cómo funcionan las capas de detección de ESET LiveGuard Advanced](#).

Dashboard

El Dashboard es un conjunto de widgets que ofrecen una descripción general de las actividades de seguridad de Microsoft 365. El Dashboard aporta información básica en cada una de las pestañas de información general (Descripción general, Exchange Online, OneDrive, grupos del equipo, sitios de SharePoint, Gmail, Google Drive y ESET LiveGuard Advanced). **Descripción general** es la pantalla principal del Dashboard que ve cada vez que inicia sesión en la consola de ESET Cloud Office Security. Muestra información general y estadística.

i El intervalo de actualización del Dashboard es de 10 minutos. Si no ve la información más reciente en su Dashboard, presione **F5** para actualizar manualmente.

Para ver estadísticas del Dashboard, use los filtros en la parte superior para elegir el **Periodo de tiempo** aplicable (últimas 24 horas, últimos 7, 30 o 90 días) y el **Inquilino**. En las pestañas de información general **Exchange Online**, **OneDrive**, **grupos del equipo**, **sitios de SharePoint**, **Gmail**, **Google Drive** y **ESET LiveGuard Advanced** pueden verse gráficos y estadísticas de detección adicionales. Estas son estadísticas, como la cantidad de correos electrónicos y archivos explorados, y la cantidad de spam/phishing/malware detectados. En los gráficos se muestra el tráfico para cada tipo de detección: spam, malware y phishing.

Ocasionalmente, puede aparecer la barra de anuncios. Los colores indican el tipo de anuncio (azul = novedades; amarillo = alerta; rojo = advertencia).

Use las pestañas del Dashboard para alternar entre los paneles de vistas:



[Información general](#)

muestra

- cantidad de inquilinos y uso de licencias
- estadísticas por cada inquilino:

O Cantidad total de usuarios/usuarios sin protección

O Principales destinatarios de spam/phishing/malware

O Principales cuentas de OneDrive sospechosas

O Principales grupos del equipo sospechosos

O Principales sitios de SharePoint sospechosos

exploración en profundidad

- haga clic en el mosaico Cantidad total de usuarios para abrir la sección [Usuarios](#)
- haga clic en un usuario de la sección de estadísticas (spam/phishing/malware/OneDrive) para ver las [Detecciones](#) pertinentes o haga clic en un grupo o sitio para ver detecciones y más información sobre el grupo del equipo o el sitio de SharePoint.

[Exchange Online](#)

muestra

- cantidad total de correos electrónicos explorados
- estadísticas de correos electrónicos de spam, malware y phishing detectados
- gráficos que representan el tráfico de spam, malware y phishing

Los mosaicos son interactivos. Haga clic en un mosaico de su interés y acceda a la sección correspondiente de la consola ESET Cloud Office Security. Por ejemplo, se abre la sección [Registros de la exploración](#) con los historiales de registros pertinentes.

[OneDrive](#)

muestra

- la cantidad de usuarios protegidos
- cantidad total de archivos explorados
- estadísticas de malware detectado
- un gráfico que representa el tráfico de malware

Los mosaicos son interactivos. Haga clic en un mosaico de su interés y acceda a la sección correspondiente de la consola ESET Cloud Office Security. Por ejemplo, se abre la sección [Registros de la exploración](#) con los historiales de registros pertinentes.

[Grupos del equipo](#)

muestra

- la cantidad de grupos protegidos
- cantidad total de archivos explorados
- estadísticas de malware detectado
- un gráfico que representa el tráfico de malware

Los mosaicos son interactivos. Haga clic en un mosaico de su interés y acceda a la sección correspondiente de la consola ESET Cloud Office Security. Por ejemplo, se abre la sección [Registros de la exploración](#) con los historiales de registros pertinentes.

[Sitios de SharePoint](#)

muestra

- la cantidad de sitios protegidos
- cantidad total de archivos explorados
- estadísticas de malware detectado
- un gráfico que representa el tráfico de malware

Los mosaicos son interactivos. Haga clic en un mosaico de su interés y acceda a la sección correspondiente de la consola ESET Cloud Office Security. Por ejemplo, se abre la sección [Registros de la exploración](#) con los historiales de registros pertinentes.

[Gmail](#)

muestra

- cantidad total de correos electrónicos explorados
- estadísticas de correos electrónicos de spam, malware y phishing detectados
- gráficos que representan el tráfico de spam, malware y phishing

Los mosaicos son interactivos. Haga clic en un mosaico de su interés y acceda a la sección correspondiente de la consola ESET Cloud Office Security. Por ejemplo, se abre la sección [Registros de la exploración](#) con los historiales de registros pertinentes.

[Google Drive](#)

muestra

- la cantidad de usuarios protegidos
- cantidad total de archivos explorados
- estadísticas de malware detectado
- un gráfico que representa el tráfico de malware

Los mosaicos son interactivos. Haga clic en un mosaico de su interés y acceda a la sección correspondiente de la consola ESET Cloud Office Security. Por ejemplo, se abre la sección [Registros de la exploración](#) con los historiales de registros pertinentes.

[ESET LiveGuard Advanced](#)

muestra

- archivos enviados (el recuento incluye duplicados y el número puede ser mayor que los archivos únicos)
- cantidad de detecciones
- tiempo promedio de análisis
- un gráfico que representa los archivos enviados
- propietarios de los principales archivos enviados
- tipos de archivos enviados

Los mosaicos son interactivos. Haga clic en un mosaico de su interés y acceda a la sección correspondiente de la consola ESET Cloud Office Security. Por ejemplo, se abre la sección [Registros de la exploración](#) con los historiales de registros pertinentes.

Usuarios

La entidad central que protege ESET Cloud Office Security es la cuenta del usuario. Haga doble clic en un usuario para buscar información de utilidad, como descripción general, configuración definida por políticas, lista de políticas asignadas al usuario y detecciones para Gmail, Google Drive, Exchange Online y OneDrive. También puede elegir qué usuarios se protegerán o no. Se ordenan los usuarios en grupos y cada grupo es un inquilino de Microsoft 365 que contiene sus usuarios. Para simplificar la búsqueda de un usuario específico dentro de un grupo, puede filtrar con múltiples criterios.

i Los usuarios sin licencia de Microsoft 365 no se mostrarán en la consola de ESET Cloud Office Security de manera predeterminada. Esto incluye buzones de correo compartidos sin una licencia de Microsoft 365. Si quiere ver y administrar todos los usuarios de Microsoft 365, vaya a [Configuración](#) y deshabilite la opción Usuarios con licencia de Microsoft 365.

Estado de protección:

Estado	Descripción
 Desprotegido	Un usuario no cuenta con protección actualmente.
 Protegido automáticamente	Usuario protegido con protección automática.
 Pendiente	Estado de transición que tiene lugar durante el proceso de proteger a un usuario. Una vez que finaliza, el estado del usuario cambia a Protegido.
 Protegido	El buzón de correo y OneDrive del usuario cuentan con la protección de una política predeterminada o personalizada .
 ADVERTENCIA	Ocurrió un error en el proceso de proteger a un usuario. El error pudo haberse producido de los recursos, Mailbox o OneDrive. Es probable que ambos recursos no estén disponibles para el usuario. Verifique si el usuario tiene una licencia válida de Microsoft 365 asignada.

Navegue por el árbol para ver los usuarios de un inquilino o grupo específico. Para ver todos los usuarios de cada

inquilino o grupo, haga clic en **Todos**.

Para obtener información más detallada, haga doble clic en un usuario, o bien, en el ícono  y seleccione una acción (**Mostrar detalles**, **Proteger** o **No proteger**). Haga clic en un usuario para abrir la ventana **Mostrar detalles**, que está compuesta por cuatro partes:

Acción	Uso
Información general	Muestra información básica sobre el usuario que se cargó desde Microsoft 365 (correo electrónico, grupo, perfil de trabajo, etc.). Además, se muestra un estado de protección actual para el buzón de correo y OneDrive.
Configuración	Contiene una lista de solo lectura de las configuraciones y las políticas asignadas para este usuario. Cambie entre las pestañas para ver la configuración o una lista de las políticas asignadas. No puede modificar la configuración ni asignar políticas a usuarios; en su lugar, vaya a la sección Políticas .
Detecciones	Muestra todas las detecciones para esta cuenta de usuario (Gmail, Google Drive, Exchange Online o OneDrive).
Cuarentena	Muestra todos los correos electrónicos y almacenamiento de archivos puestos en cuarentena de este usuario. También puede usar una acción: Liberar, Descargar o Eliminar archivos o correos electrónicos en cuarentena.

Puede filtrar los usuarios usando varios criterios. Haga clic en **Agregar filtro** y seleccione un tipo de filtro del menú desplegable o introduzca una secuencia (se repite al combinar varios criterios):

Agregar filtro	Uso
Estado de protección	Seleccione el estado Protegido, No protegido, Advertencia o Pendiente de un usuario.
Protegido automáticamente	Mostrar solo los usuarios protegidos automáticamente.
Nombre	Escriba un nombre de usuario válido.
Correo electrónico	Escriba un correo electrónico de usuario válido.
Tipo	Seleccione el tipo de usuario (Desconocido, Usuario, Vinculado, Buzón compartido, Sala, Equipo, Otros).

[Proteger a los usuarios](#)

1. Seleccione los **usuarios** que se protegerán y haga clic en **Proteger**.
2. Seleccione el **grupo de licencias** cargado desde ESET Business Account y haga clic en **Aceptar**. La política predeterminada ahora protege a los usuarios seleccionados.
3. De ser necesario, especifique una política personalizada para los usuarios en la sección [Políticas](#).

[Desproteger usuarios](#)

Seleccione los **usuarios** que no se protegerán y haga clic en **No proteger**.

Equipos y sitios

ESET Cloud Office Security ofrece protección para grupos del equipo o sitios de SharePoint.

Cambie entre las pestañas de grupos del equipo y sitios de SharePoint. Muestra una lista de grupos del equipo o sitios de SharePoint para cada inquilino.

Grupos del equipo

Muestra objetos que son tipos de grupo de Microsoft 365, incluidos el sitio predeterminado del equipo de SharePoint y OneDrive:

- nombre
- estado
- correo electrónico
- inquilino

Para proteger a los grupos del equipo, asegúrese de que al menos un miembro de los registros de la exploración sea un usuario protegido por ESET Cloud Office Security. Cada grupo de Microsoft 365 tiene un sitio de equipo de SharePoint predeterminado y OneDrive, que también están protegidos.

Sitios de SharePoint

Muestra todos los sitios de origen de SharePoint que no están asociados al grupo de Microsoft 365:

- nombre
- estado
- URL
- inquilino

Los sitios de SharePoint se protegen automáticamente, incluidos sus subsitios (no se muestran).

Para obtener información más detallada, haga clic en un grupo del equipo o en un sitio de SharePoint para abrir la ventana **Mostrar detalles** que consta de cuatro partes:

Acción	Uso
Información general	Muestra la información necesaria sobre los grupos del equipo o sitios de SharePoint cargados desde Microsoft 365 (correo electrónico, propietario, miembros, autor, URL, etc.). Además, se muestra el estado de protección actual del grupo del equipo o el sitio de SharePoint.
Configuración	Contiene una lista de solo lectura de las configuraciones y las políticas asignadas. Cambie entre las pestañas para ver la configuración o una lista de las políticas asignadas. No puede modificar la configuración ni asignar políticas; en su lugar, vaya a la sección Políticas .
Detecciones	Mostrar todas las detecciones del grupo del equipo o del sitio de SharePoint.
Cuarentena	Mostrar todos los archivos en cuarentena. También puede usar una acción: Liberar, Descargar o Eliminar archivos en cuarentena.

Haga clic en **Agregar filtro** para filtrar los grupos del equipo o los sitios de SharePoint.

Detecciones

Muestra una lista de todas las detecciones realizadas por ESET Cloud Office Security. Cambie entre Gmail, Google Drive, Exchange Online, OneDrive, grupos del equipo y sitios de SharePoint utilizando las pestañas. Observe la información en cada detección; por ejemplo, los archivos que se cargaron en un grupo de Team en la ficha Grupos del equipo.

Haga clic en el icono  para abrir una barra lateral con un resumen de un registro específico (detección). Para obtener información más detallada, haga clic en el icono  y seleccione **Mostrar detalles**.

Navegue por el árbol para ver las detecciones solo de un inquilino o grupo específico. Para ver todas las detecciones de cada inquilino o grupo, haga clic en **Todo**. Para simplificar la búsqueda de una detección específica, puede filtrar y aplicar múltiples criterios. Haga clic en **Agregar filtro** y seleccione el tipo de filtro del menú desplegable o introduzca una secuencia (se repite al combinar criterios):

Agregar filtro	Uso
Ocurrió desde	Especifica un rango "Fecha desde".
Ocurrió hasta	Especifica un rango "Fecha hasta".
Asunto	Se aplica a los mensajes que contengan o no una cadena específica (o una expresión regular) en el asunto.
ID del mensaje	Filtre los mensajes de correo electrónico por una ID del mensaje exclusiva al buscar un mensaje específico, especialmente en registros grandes con muchos mensajes o intentos de entrega múltiple.
Desde	Filtre los mensajes por un remitente específico.
Hasta	Filtra mensajes por destinatarios.
Buzón de correo	Se aplica a los mensajes ubicados en un buzón de correo específico.
Explorar resultado	Seleccione una de las siguientes opciones: Malware,  Malware (detectado por ESET LiveGuard Advanced), Phishing o Spam.
Acción	Seleccione una de las acciones disponibles.
Equipo	Escriba un nombre de equipo válido.
Sitio	Escriba un nombre de sitio válido.
Objeto	Escriba un nombre de objeto válido.
Detección	Escriba un nombre de detección válido.
Hash	Escriba un hash de detección válido.

Al hacer clic en el icono , la opción **Quitar de la lista blanca** estará disponible en caso de que haya colocado un archivo previamente en la lista blanca al liberarlo de la [Cuarentena](#) para el mismo usuario. Use esta opción para eliminar un archivo de la lista blanca. Todos dichos archivos futuros se colocarán en cuarentena.

 El período de conservación para las detecciones es de 90 días. Se eliminarán de manera permanente los registros que superen los 90 días.

Denunciar falso positivo (FP)/falso negativo (FN)

Puede denunciar detecciones de FP y FN en forma manual para spam, phishing o malware mediante el envío de una muestra a los laboratorios de ESET para realizar un análisis. Direcciones de correo electrónico para enviar las muestras:

Spam: envíe un correo electrónico a nospam_ecos@eset.com para correos electrónicos marcados como spam de manera incorrecta o a spam_ecos@eset.com para spam no detectados con el mensaje original como adjunto con formato *.eml* o *.msg*.

Phishing: para denunciar una clasificación de falsos negativos o falsos positivos de phishing, cree un nuevo mensaje de correo electrónico a samples@eset.com con 'phishing email' en el asunto e incluya el correo electrónico de phishing como adjunto con formato *.eml* o *.msg*.

Malware: para una clasificación de falsos negativos o falsos positivos de malware, cree un nuevo mensaje de

correo electrónico a samples@eset.com con *'False positive'* o *'Suspected infection'* en el asunto e incluya los archivos comprimidos con formato *.zip* o *.rar* como adjunto.

Informes

Los informes de ESET Cloud Office Security lo mantienen informado con una descripción general de las estadísticas de protección de ESET Cloud Office Security. Puede elegir entre dos tipos de informes, informes estadísticos o informes de Cuarentena de correo.

Los informes estadísticos contienen información sobre la protección de Gmail, Google Drive, Exchange Online, OneDrive, grupos del equipo y sitios de SharePoint, la cantidad de correos electrónicos analizados, archivos, malware, phishing y spam detectados durante el periodo especificado. Los informes se pueden generar y descargar manualmente en formato *PDF* o *CSV*, o programarse y enviarse a los destinatarios seleccionados por correo electrónico. El formato de salida *PDF* presenta los datos en un formato de gráfico, muestra el promedio a largo plazo para su comparación e incluye información sobre el tráfico de cada tipo de protección, los principales destinatarios de malware, phishing y spam.

El informe de Cuarentena de correo contiene una lista de los objetos que se han puesto en cuarentena recientemente. El informe se envía por correo electrónico a los destinatarios seleccionados. Los destinatarios pueden liberar mensajes de spam (si se consideran seguros o legítimos) al hacer clic en el vínculo **Liberar**. Solo se aplica al spam; no se pueden liberar otros tipos de objetos en cuarentena.

Puede acceder a las estadísticas por correo electrónico sin necesidad de iniciar sesión en la consola ESET Cloud Office Security. Configure y programe informes recurrentes y especifique destinatarios de correo electrónico. Además, puede generar estadísticas de informes inmediatamente desde la consola ESET Cloud Office Security. Seleccione un informe existente (también puede ser un informe programado) y haga clic en **Generar y Descargar**. Hacer clic con el botón derecho en el menú desplegable también funciona. Puede crear fácilmente una nueva plantilla de informe con una configuración personalizada.

Nuevo informe

Haga clic en Nuevo informe para abrir un asistente de plantilla de informes y especificar la configuración personalizada. Ingrese un nombre y una descripción para el informe.

Idioma

Elija el idioma que desee en el menú desplegable. El informe se generará en el idioma seleccionado.

Tipo

Seleccione el tipo que desea incluir en las estadísticas.

Informes estadísticos

Cree informes programados o a demanda que consten de información según las opciones que elija.

Informes de la cuarentena del correo

Para informar a los usuarios sobre los mensajes de correo electrónico que pasaron a cuarentena recientemente, envíe correos electrónicos de notificación a los usuarios seleccionados. Puede asignar uno o varios destinatarios o un grupo. Elija un intervalo para los informes, y la fecha y la hora de inicio. Si se trata de un informe repetido, elija cuándo debe finalizar (en una fecha, después de varias ocurrencias, o nunca). El informe de Cuarentena de correo

solo se activará cuando hay nuevos elementos. Los destinatarios del informe pueden liberar mensajes de spam (si se consideran seguros o legítimos) al hacer clic en el vínculo Liberar (se abre una ventana de confirmación en un navegador web). El mensaje de spam liberado se envía en un correo electrónico independiente como archivo adjunto.

Inquilino

Esta opción está disponible para un entorno de varios inquilinos. Puede seleccionar varios inquilinos para los cuales generar estadísticas. El informe se generará para cada inquilino por separado y se entregará en un correo electrónico de informe ESET Cloud Office Security con varios archivos adjuntos.

Período

Defina el período en el que desea que se muestren los resultados (últimas 24 horas, semana, mes). Cuando selecciona Personalizado, puede especificar un rango (Fecha desde y Fecha hasta).

Salida

Seleccione el formato de archivo adecuado; puede elegir *PDF* o *CSV*. El formato *PDF* incluye los datos que aparecen en los gráficos. *CSV* es adecuado como datos sin procesar. Los informes se recopilarán de acuerdo con las opciones especificadas. Si realiza múltiples selecciones (Exchange Online, OneDrive, grupos del equipo, sitios de SharePoint, Gmail, Google Drive), el archivo de salida podría ser un archivo en un formato ZIP que contiene archivos de informe *PDF* o *CSV*.

Etiqueta blanca

Si necesita que el logo de su empresa aparezca en el informe, habilite esta función. Tiene la opción de usar el encabezado del informe de marca compartida que muestra su logo junto con el logo de ESET o solo el suyo. Cargue el logo en formato *PNG* o *JPEG*.

Programado

Use las tareas programadas para que los informes se generen en una fecha y una hora especificadas, también como evento recurrente. Los informes programados se entregan a destinatarios seleccionados que recibirán el correo electrónico del informe ESET Cloud Office Security con archivos adjuntos.

Repetir

Elija si desea que el informe se genere una o varias veces:

- **Una vez:** el informe se realizará solo una vez.
- **Diariamente:** el informe se generará y entregará reiteradamente, todos los días (a menos que especifique que la recurrencia finalice tras las ocurrencias).
- **Semanalmente:** el informe se generará y entregará reiteradamente los días de la semana seleccionados.
- **Mensualmente:** el informe se generará y entregará una vez al mes en un día seleccionado.

Comenzar desde

Elija la fecha de inicio de los informes.

Finaliza

Seleccione cuándo finaliza el intervalo de recurrencia.

Destinatarios

Especifique la dirección de correo electrónico del destinatario del informe y presione Intro para confirmar. Repita para agregar varios destinatarios.

Para obtener información o acciones detalladas, haga clic en el ícono  y seleccione una acción:

Acción	Uso
Mostrar detalles	Muestra información detallada sobre un informe.
Generar & Descargar	Haga clic en Generar y Descargar y elija <i>PDF</i> o <i>CSV</i> . El formato <i>PDF</i> incluye los datos mostrados en gráficos. <i>CSV</i> es adecuado como datos sin procesar. Los informes se recopilarán de acuerdo con las opciones especificadas. Si seleccionó tanto datos de Exchange Online como de OneDrive, grupos del equipo o sitios de SharePoint, el archivo de salida podría ser un archivo en un formato <i>ZIP</i> que contiene archivos de informe <i>PDF</i> o <i>CSV</i> .
Editar	Edite la configuración de un informe existente.
Eliminar	Elimine el informe seleccionado por completo.

Para filtrar los informes, haga clic en **Agregar filtro** y seleccione un tipo de filtro del menú desplegable o introduzca una secuencia (repetir al combinar varios criterios):

Agregar filtro	Uso
Nombre	Escriba el nombre parcial o completo del informe.
Programado	Seleccione No programado, Una vez, Diariamente, Semanalmente o Mensualmente.
Datos	Seleccione Exchange Online, OneDrive, grupos del equipo o sitios de SharePoint para filtrar por datos.

Cuarentena

Administración simple de los objetos (correos electrónicos y archivos) que ESET Cloud Office Security puso en cuarentena. Cambie entre Gmail, Google Drive, Exchange Online, OneDrive, grupos del equipo y sitios de SharePoint utilizando las pestañas. Puede ver información relevante sobre cada objeto.

Haga clic en el ícono  para abrir una barra lateral con un resumen de un objeto específico. Para obtener información más detallada, haga clic en el ícono  y seleccione **Mostrar detalles**.

Navegue por el árbol para ver las detecciones solo de un inquilino o grupo específico. Para ver todas las detecciones de cada inquilino o grupo, haga clic en **Todo**.

Inspeccione los mensajes de correo electrónico o los archivos puestos en cuarentena, y realice alguna acción (**Eliminar** o **Liberar**). También puede **descargar** el archivo original o el archivo protegido con contraseña en el formato *.zip*.

i Cuando considera una detección como no maliciosa (falso positivo), puede **Liberar** un archivo de la Cuarentena. El archivo liberado se coloca automáticamente en una lista blanca, según el hash. Todas las ocurrencias futuras del mismo archivo, para el mismo usuario, no se detectarán como sospechosas y no se colocarán en cuarentena. La colocación automática en listas blancas se realiza por usuario. Para otros usuarios, el mismo archivo aún se detectará como sospechoso o en cuarentena. Puede eliminar un archivo de la lista blanca en la lista [Detecciones](#) usando la opción **Eliminar de la lista blanca**.

Haga clic en el ícono  y seleccione una acción:

Acción	Uso
Mostrar detalles	Muestra más información detallada sobre el mensaje de correo electrónico puesto en cuarentena.
Liberar (correo electrónico o archivos)	Libera correos electrónicos a los destinatarios originales con el formato de correo electrónico de notificación desde Cuarentena con el mensaje original como adjunto. Si se trata de un elemento de OneDrive, se cargará el archivo a su ubicación original en OneDrive del usuario. Si se libera un archivo de un grupo del equipo o un sitio de SharePoint, el archivo aparecerá de nuevo en su ubicación original. El archivo liberado se coloca automáticamente en una lista blanca, según el hash. Esto impide que el archivo se vuelva a poner en cuarentena.
Eliminar	Elimina el elemento de la cuarentena.
Descargar archivo original	Se descarga el archivo no protegido en su formato original.
Descargar archivo protegido con contraseña	Se descarga el archivo protegido con contraseña.
Enviar muestra	El cuadro de diálogo de envío de muestras le permite enviar un archivo sospechoso o spam a ESET para analizar. Elija un Motivo por el cual se envía la muestra del menú desplegable.

Para simplificar la búsqueda de un objeto específico puesto en cuarentena, puede filtrar con múltiples criterios. Haga clic en **Agregar filtro** y seleccione el tipo de filtro del menú desplegable o introduzca una secuencia (se repite al combinar criterios):

Agregar filtro	Uso
Ocurrió desde	Especifica un rango "Fecha desde".
Ocurrió hasta	Especifica un rango "Fecha hasta".
Asunto	Se aplica a los mensajes que contengan o no una cadena específica (o una expresión regular) en el asunto.
ID del mensaje	Filtre los mensajes de correo electrónico por una ID del mensaje exclusiva al buscar un mensaje específico, especialmente en registros grandes con muchos mensajes o intentos de entrega múltiple.
Desde	Filtre los mensajes por un remitente específico.
Hasta	Filtra mensajes por destinatarios.
Buzón de correo	Se aplica a los mensajes ubicados en un buzón de correo específico.
Explorar resultado	Seleccione una de las siguientes opciones: Malware,  Malware (detectado por ESET LiveGuard Advanced), Phishing o Spam.
Equipo	Escriba un nombre de equipo válido.
Objeto	Escriba un nombre de objeto válido.
Sitio	Escriba un nombre de sitio válido.

i El período de conservación para los objetos puestos en cuarentena es de 30 días. Se eliminarán de manera permanente los objetos que superen los 30 días.

Registros de la exploración

Menciona todos los resultados de la exploración por ESET Cloud Office Security. Los registros son similares a las [detecciones](#), pero también puede incluir en la lista objetos limpios (activar la configuración de Registrar todos los objetos en las políticas). Cambie entre Gmail, Google Drive, Exchange Online, OneDrive, grupos del equipo, sitios de SharePoint y Archivos enviados mediante las pestañas. Puede ver una mucha información de cada detección. Archivos enviados es una lista de los archivos enviados a ESET LiveGuard Advanced para su análisis.

Haga clic en el icono  para abrir una barra lateral con un resumen de un registro específico. Para obtener información más detallada, haga clic en el icono  y seleccione **Mostrar detalles**.

Navigate por el árbol para ver los registros solo de un inquilino o grupo específico. Para ver todas las detecciones de cada inquilino o grupo, haga clic en **Todo**.

i Si el resultado de una exploración es **No explorado**, el motivo puede variar. Consulte [Limitaciones](#) para conocer los detalles.

Cuando hace clic en el ícono del engranaje  situado en la esquina superior derecha para acceder al menú contextual **Exportar a CSV**, puede exportar la tabla a formato *CSV* y utilizarla en otras aplicaciones para trabajar con la lista.

Para simplificar la búsqueda de un registro específico, puede filtrar y aplicar múltiples criterios. Haga clic en **Agregar filtro** y seleccione el tipo de filtro del menú desplegable o introduzca una secuencia (se repite al combinar criterios):

Agregar filtro	Uso
Ocurrió desde	Especifica un rango "Fecha desde".
Ocurrió hasta	Especifica un rango "Fecha hasta".
Fuente de datos	Seleccione una de las siguientes opciones: Exchange Online, OneDrive, grupo del equipo y sitio de SharePoint.
Buzón de correo	Se aplica a los mensajes ubicados en un buzón de correo específico.
Desde	Filtre los mensajes por un remitente específico.
Hasta	Filtra mensajes por destinatarios.
Asunto	Se aplica a los mensajes que contengan o no una cadena específica en el asunto.
ID del mensaje	Filtre los mensajes de correo electrónico por una ID del mensaje exclusiva al buscar un mensaje específico, especialmente en registros grandes con muchos mensajes o intentos de entrega múltiple.
Explorar resultado	Seleccione una de las siguientes opciones: Malware,  Malware (detectado por ESET LiveGuard Advanced), phishing, spam, limpio, no explorado, error o deshabilitado.
Acción	Seleccione una de las acciones disponibles.
Propietarios	Escriba un nombre de propietario válido.
Objeto	Escriba un nombre de objeto válido.
Detección	Escriba un nombre de detección válido.
Hash	Escriba un hash de detección válido.

Agregar filtro	Uso
Equipo	Escriba un nombre de equipo válido.
Sitio	Escriba un nombre de sitio válido.

i Los registros tienen un período de retención de 90 días. Se eliminarán de manera permanente los registros que superen los 90 días. Si tiene una política que usa la función **Registrar todos los objetos**, la conservación para los registros con un resultado de exploración **Limpio** es de 3 días. Los resultados limpios de exploraciones superiores a 3 días se eliminarán de manera permanente.

Políticas

Las organizaciones más grandes suelen tener múltiples departamentos y desean configurar distintos niveles de protección para cada unidad organizacional. ESET Cloud Office Security proporciona configuraciones de protección basadas en políticas que puede personalizar en función de sus necesidades y asignar a usuarios y grupos de usuarios, inquilinos o grupos del equipo o sitios de SharePoint seleccionados.

Para agregar criterios de filtrado, haga clic en **Agregar filtro** y seleccione el elemento aplicable **Nombre** y escriba un nombre de política válido. El árbol de políticas muestra a los inquilinos y sus grupos de usuarios, grupos del equipo o sitios de SharePoint, incluido un grupo **Sin asignar** que contiene políticas personalizadas que no se encuentran asignadas a ningún destino.

Puede agregar una nueva política o modificar una política existente y sus configuraciones:

- Haga clic en **Políticas > Nueva política**.
- Haga clic en **Nombre** y **Descripción** para una nueva política.
- Seleccione un destino y configure una política para:
 - **Inquilinos** – Configurar la protección de Gmail, Google Drive, Exchange Online, OneDrive, los sitios de SharePoint y grupos del equipo, y asignarla a los inquilinos seleccionados
 - **Usuarios** – Configurar la protección de Gmail, Google Drive, Exchange Online y OneDrive y asignarla a los usuarios seleccionados o a un grupo de usuarios
 - **Grupos del equipo** – Configurar la protección de grupos del equipo y asignarla a los grupos de equipo seleccionados
 - **Sitios de SharePoint** – Configurar la protección de los sitios de SharePoint y asignarla a los sitios seleccionados
- Personalice la **Configuración** de protección para [Exchange Online](#), [Gmail](#), [OneDrive](#), [Google Drive](#), [grupos del equipo](#), [sitios de SharePoint](#) o [ESET LiveGuard Advanced](#) y haga clic en **Siguiente**.
- Haga clic en **Asignar** y elija el destino al que se asignará la política.
- Haga clic en **Guardar cambios** para guardar la configuración de la política.

 [Principios de las políticas](#)

Política predeterminada

- Aplica a todos los usuarios (protegidos y sin protección)
- No se pueden modificar ni eliminar

La política personalizada puede asignarse a:

- **Usuarios:** se aplica a usuarios concretos seleccionados manualmente
- **Grupos:** se aplica a todos los miembros del grupo de usuarios
- **Inquilinos:** política que se aplica a todas las entidades del inquilino
- **Grupos de equipos:** se aplica a un grupo del equipo
- **Sitios de SharePoint:** se aplica a un sitio de SharePoint

La política personalizada asignada a un **inquilino** o **grupo** se combina con la política predeterminada.

La **política de inquilinos**, la **política de grupos**, la **política de grupos del equipo** o la **política de sitios de SharePoint** personalizadas tienen prioridad sobre la política predeterminada

La política personalizada asignada a un **usuario** se combina con la política de **inquilinos, grupos, grupos del equipo** o **sitios de SharePoint** y con la política predeterminada

Una política de **usuario** personalizada tiene prioridad sobre una política de Inquilino o Grupo y una predeterminada. No obstante, cuando un usuario carga un archivo en un grupo de Team o en un sitio de SharePoint, se aplica la política para el grupo del equipo o el sitio de SharePoint.

Pueden asignarse varias **políticas personalizadas** a los usuarios e inquilinos, pero la política efectiva se calcula en función de la prioridad (orden).

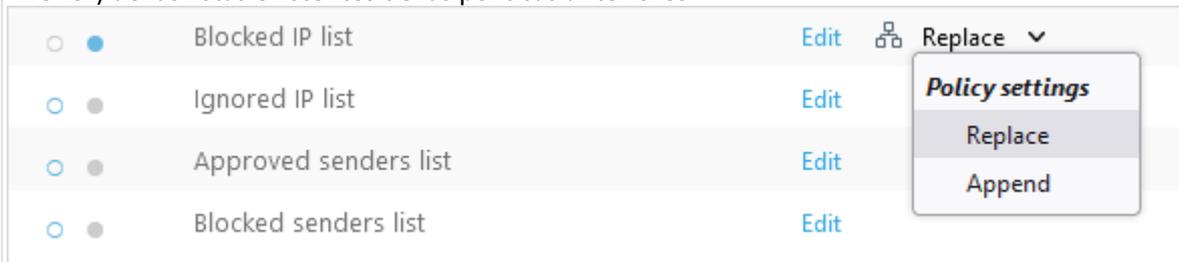
 [Configuración de listas antispam al fusionar políticas](#)

La opción de fusión se aplica a las [listas antispam](#) y a la configuración de [Notificar al administrador](#) (direcciones de correos electrónicos de notificación mediante Anti-malware y Anti-phishing).

Si tiene varias políticas con listas antispam (listas de direcciones IP, dominios o direcciones de correo electrónico aprobadas, bloqueadas e ignoradas) o direcciones de administrador de anti-malware y anti-phishing para correos electrónicos de notificación, elija la estrategia de fusión:

Reemplazar: mantenga solo las entradas de la lista nuevas (opción predeterminada). Las nuevas entradas de la lista de la política actual reemplazan las listas de las políticas anteriores.

Adjuntar: amplíe las listas de las políticas anteriores adjuntando entradas nuevas. Fusione las listas de las políticas anteriores con las nuevas entradas de la política actual. Las nuevas entradas se colocan al final (parte inferior) de las listas existentes de las políticas anteriores.



i Antes de que la opción de fusión estuviera disponible, el comportamiento predeterminado era **Reemplazar**. Si ya utiliza políticas con listas antispam específicas, puede conservar la opción predeterminada **Reemplazar** o cambiarla por **Adjuntar**, si así lo prefiere.

Cree una nueva política con una lista antispam definida y seleccione la opción de fusión (suponiendo que haya políticas existentes con listas antispam).

1. Haga clic en **Políticas > Nueva política**.
2. Escriba un **Nombre** y una **Descripción** para la nueva política, seleccione **Inquilinos** como destino y haga clic en **Siguiente**.
3. Expanda **Antispam de Exchange Online** y haga clic en **Editar** junto a la lista de IP bloqueadas.
- ✓ 4. Haga clic en **Agregar**, escriba la dirección IP, pulse la tecla **Enter** para completar la acción (también puede importar la lista desde un archivo) y, a continuación, hacer clic en **Guardar cambios**.
5. Elija **Adjuntar** como opción de fusión en el menú desplegable y haga clic en **Siguiente**.
6. Haga clic en **Asignar**, elija **Asignar a inquilinos** en el menú desplegable, marque la casilla de verificación situada junto al inquilino y haga clic en **Aceptar**.
7. Haga clic en **Guardar cambios** para terminar el proceso.

i Para reordenar la prioridad de las políticas, haga clic en **Cambiar orden**. Seleccione una o varias políticas, y haga clic en **Aplicar antes** o **Aplicar más tarde** para cambiar su prioridad. Las políticas se aplican a nivel global (independientemente de la asignación, es decir, inquilino, grupo o usuario) en el orden especificado en sentido descendente. La política predeterminada se aplica siempre primero.

Para realizar las siguientes acciones, seleccione la política y haga clic en el icono :

Acción	Uso
Mostrar detalles	Muestra información detallada sobre una política creada, la configuración y destinatarios de las políticas asignadas.
Editar	Edita la configuración de una política existente.
Asignar	Seleccione los usuarios, los inquilinos, los grupos del equipo o los sitios de SharePoint a los que se aplica la política.
Duplicar	Cree una política nueva basada en la plantilla seleccionada. Será necesario que la política duplicada tenga otro nombre.
Eliminar	Quita la política seleccionada por completo.

Cree una política de inquilino personalizada para ver todos los resultados de la exploración (incluidos los limpios) en [Registros de la exploración](#). La política de inquilino aplica a todos los usuarios (protegidos y sin protección).

1. Haga clic en **Políticas > Nueva política**.
2. Escriba un **Nombre** y una **Descripción** para la nueva política, seleccione **Inquilinos** como destino y haga clic en **Siguiente**.
3. Amplíe la **configuración general de Exchange Online** y haga clic en el botón de alternancia para habilitar **Registrar todos los objetos**.
- ✓ 4. Amplíe la **configuración general de OneDrive** y haga clic en el botón de alternancia para habilitar **Registrar todos los objetos**.
5. Amplíe la **configuración general de grupo del equipo** y haga clic en el botón de alternancia para habilitar **Registrar todos los objetos**.
6. Amplíe la **configuración general de los sitios de SharePoint** y haga clic en el botón de alternancia para habilitar **Registrar todos los objetos**. Luego, haga clic en **Siguiente**.
7. Haga clic en **Asignar**, seleccione la casilla de verificación junto al inquilino y, luego, haga clic en **Aceptar**.
8. Haga clic en **Guardar cambios** para terminar el proceso.

Crear una política personalizada para usuarios específicos con configuraciones avanzadas que afectará la manera en que se abordan el malware, spam y phishing. Habiendo implementado esta política, se eliminarán los archivos adjuntos de correos electrónicos que contienen malware, se moverán los mensajes de spam a la carpeta de correo electrónico no deseado del usuario, se etiquetarán los asuntos de los correos electrónicos de phishing y se pondrán en cuarentena, y los contenidos de archivos de malware ubicados en OneDrive se reemplazarán con texto simple para evitar provocar daños.

1. Haga clic en **Políticas > Nueva política**.
2. Escriba un **Nombre** y una **Descripción** para la nueva política, seleccione **Usuarios** como destino y haga clic en **Siguiente**.
3. Amplíe **Protección contra malware de Exchange Online** y use el menú desplegable junto a **Cuando se detectan elementos** para seleccionar **Eliminar adjunto**.
- ✓ 4. Amplíe **Protección contra spam de Exchange Online** y use el menú desplegable junto a **Cuando se detectan elementos** para seleccionar **Mover a correo no deseado**.
5. Amplíe **Protección Anti-Phishing de Exchange Online** y haga clic en el botón de alternancia para habilitar **Etiquetar asunto**. También puede cambiar el **texto del asunto de la etiqueta** para personalizarlo.
6. Amplíe **Protección contra malware de OneDrive Online**, use el menú desplegable junto a **Cuando se detectan elementos** para seleccionar **Reemplazar** y haga clic en **Siguiente**.
7. Haga clic en **Asignar**, seleccione las casillas de verificación junto a los usuarios a los cuales quiere aplicarles la política y haga clic en **Aceptar**. Si un usuario tiene una política personalizada existente aplicada, se sobrescribirá con la nueva política.
8. Haga clic en **Guardar cambios** para terminar el proceso.

Configuración de la protección para Exchange Online

En esta sección, se aporta información sobre cómo cambiar las opciones y la configuración generales, de protección contra malware, contra spam o Anti-Phishing de Exchange Online.

↗ [Configuración general de Exchange Online](#)

ESET LiveGrid® Comentarios sobre

Se enviarán datos al ESET Research Lab para su análisis posterior. Puede obtener más información sobre ESET LiveGrid® en el [glosario](#).

Registrar todos los objetos

Si se selecciona esta opción, todos los resultados de la exploración (incluidos los limpios) se mostrarán en [Registros de la exploración](#). La política de retención para los resultados de exploración de limpieza es de tres días. Los resultados de la exploración superiores a tres días se eliminarán de manera permanente.

[Protección contra malware de Exchange Online](#)

Habilitar protección contra malware de Exchange Online

Cuando está habilitada, esta función está activa y puede configurar opciones detalladas.

Informes y protección del aprendizaje automático

El aprendizaje automático avanzado ahora forma parte del motor de detección como una capa de protección avanzada, lo que mejora la detección. Lea lo siguiente antes de modificar un umbral (o nivel) de categoría

[Informar](#):

Cuando se detectan elementos

- **Sin acción:** no se realiza ninguna acción y el correo electrónico se entrega al destinatario
- **Mover a correo no deseado:** el correo electrónico se mueve a la carpeta correo no deseado.
- **Mover a la papelera:** el correo electrónico se mueve a la carpeta de la papelera.
- **Eliminar mensaje:** se elimina el correo electrónico.
- **Poner en cuarentena el mensaje:** el correo electrónico original se elimina y la copia del correo electrónico se almacena en cuarentena. Si decide liberar el correo electrónico de la cuarentena, se envía como un adjunto en un nuevo correo electrónico y se entrega al destinatario.
- **Eliminar archivo adjunto:** el archivo adjunto del mensaje se elimina y el mensaje se entrega sin este.
- **Reemplazar adjunto:** el adjunto se reemplaza con un archivo de texto que contiene información detallada sobre una acción tomada.
- **Colocar el archivo adjunto en cuarentena:** el archivo adjunto se elimina del correo electrónico y se pone en cuarentena

Texto de sustitución de archivo adjunto

Reemplazar el adjunto con un archivo de texto que contiene información detallada sobre una acción tomada.

Asunto de la etiqueta

Cuando esté habilitado, puede modificar plantillas añadidas al asunto de mensajes infectados.

Texto de asunto de etiqueta

Puede agregar una etiqueta personalizada a los asuntos de los mensajes afectados.

Notificar al propietario del buzón

Cuando esta opción está habilitada, el usuario recibe un correo electrónico de notificación cuando se realiza una detección.

Idioma

Elija el idioma que desee en el menú desplegable. El propietario del buzón recibirá correos electrónicos de notificación en el idioma seleccionado cuando se libera un objeto de la cuarentena de Exchange Online. Esta opción anula el idioma predeterminado del inquilino en la [configuración](#).

Notificar al administrador

Se especifica una dirección de correo electrónico (presionar Intro para agregar varias direcciones) que recibirá correos electrónicos de notificación siempre que se realice una detección.

[Protección contra spam de Exchange Online](#)

Habilitar protección contra spam de Exchange Online

Cuando está habilitada, esta función está activa y puede configurar opciones detalladas.

Cuando se detectan elementos

- **Sin acción:** no se realiza ninguna acción y el correo electrónico se entrega al destinatario
- **Mover a correo no deseado:** el correo electrónico se mueve a la carpeta correo no deseado.
- **Mover a la papelera:** el correo electrónico se mueve a la carpeta de la papelera.
- **Eliminar mensaje:** se elimina el correo electrónico.
- **Poner en cuarentena el mensaje:** el correo electrónico original se elimina y la copia del correo electrónico se almacena en cuarentena. Si decide liberar el correo electrónico de la cuarentena, se envía como un adjunto en un nuevo correo electrónico y se entrega al destinatario.

Asunto de la etiqueta

Cuando esté habilitado, puede modificar plantillas añadidas al asunto de mensajes infectados.

Texto de asunto de etiqueta

Puede agregar una etiqueta personalizada a los asuntos de los mensajes afectados.

Puede configurar listas de **Permitidos, Bloqueados e Ignorados** al especificar criterios como la dirección o el rango IP, el nombre del dominio, etc. Para agregar, modificar o eliminar criterios, haga clic en **Editar** para abrir la lista que desea administrar. De manera alternativa, puede importar su lista personalizada desde un archivo en lugar de agregar cada entrada de forma manual. Haga clic en **Importar** y busque el archivo (.txt) que contenga las entradas que desea agregar a la lista. Asimismo, si necesita exportar su lista actual a un archivo (.txt), seleccione **Exportar** desde el menú contextual.

Lista de IP aprobada	Coloca automáticamente en la lista blanca a los correos electrónicos que se originan desde direcciones IP especificadas. No se comprobará el contenido del correo electrónico.
Lista de IP bloqueada	Bloquea automáticamente los correos electrónicos que se originan desde direcciones IP especificadas.
Lista de IP ignorada	Lista de direcciones IP que se ignorarán durante la clasificación. Se comprobará el contenido del correo electrónico.
Lista de remitentes aprobados	Envía a la lista blanca los correos electrónicos que tienen su origen en un remitente o dominio específico. Para la verificación solo se utiliza una dirección de remitente o un dominio completo, en función de la siguiente prioridad: 1. Dirección SMTP "MAIL FROM" 2. Campo del encabezado de correo electrónico "Return-Path:" 3. Campo del encabezado de correo electrónico "X-Env-Sender:" 4. Campo del encabezado de correo electrónico "From:" 5. Campo del encabezado del correo electrónico "Sender:" 6. Campo del encabezado del correo electrónico "X-Apparently-From:"
Lista de remitentes bloqueados	Bloquea los correos electrónicos que tienen su origen en un remitente o dominio específico. Para la verificación se utilizan todas las direcciones de remitentes identificadas o todos los dominios: Dirección SMTP "MAIL FROM" Campo del encabezado de correo electrónico "Return-Path:" Campo del encabezado de correo electrónico "X-Env-Sender:" Campo del encabezado de correo electrónico "From:" Campo del encabezado del correo electrónico "Sender:" Campo del encabezado del correo electrónico "X-Apparently-From:"

 [Protección contra phishing de Exchange Online](#)

Habilitar protección contra phishing de Exchange Online

Cuando está habilitada, esta función está activa y puede configurar opciones detalladas.

Cuando se detectan elementos

- **Sin acción:** no se realiza ninguna acción y el correo electrónico con el adjunto malicioso se entrega al destinatario.
- **Mover a correo no deseado:** el correo electrónico se mueve a la carpeta correo no deseado.
- **Mover a la papelera:** el correo electrónico se mueve a la carpeta de la papelera.
- **Eliminar mensaje:** se elimina el correo electrónico.
- **Poner en cuarentena el mensaje:** el correo electrónico original se elimina y la copia del correo electrónico se almacena en cuarentena. Si decide liberar el correo electrónico de la cuarentena, se envía como un adjunto en un nuevo correo electrónico y se entrega al destinatario.

Asunto de la etiqueta

Cuando esté habilitado, puede modificar plantillas añadidas al asunto de mensajes infectados.

Texto de asunto de etiqueta

Puede agregar una etiqueta personalizada a los asuntos de los mensajes afectados.

Notificar al propietario del buzón

Cuando esta opción está habilitada, el usuario recibe un correo electrónico de notificación cuando se realiza una detección.

Notificar al administrador

Se especifica una dirección de correo electrónico (presionar Intro para agregar varias direcciones) que recibirá correos electrónicos de notificación toda vez que se realice una detección para un usuario de Exchange Online.

Configuración de la protección de Gmail

En esta sección, se aporta información sobre cómo cambiar las opciones y la configuración generales, de protección contra malware, contra spam o Anti-Phishing de Gmail.

[Generalidades de Gmail](#)

ESET LiveGrid® Comentarios sobre

Se enviarán datos al ESET Research Lab para su análisis posterior. Puede obtener más información sobre ESET LiveGrid® en el [glosario](#).

Registrar todos los objetos

Si se selecciona esta opción, todos los resultados de la exploración (incluidos los limpios) se mostrarán en [Registros de la exploración](#). La política de retención para los resultados de exploración de limpieza es de tres días. Los resultados de la exploración superiores a tres días se eliminarán de manera permanente.

[Protección contra malware de Gmail](#)

Habilitar protección contra malware de Gmail

Cuando está habilitada, esta función está activa y puede configurar opciones detalladas.

Informes y protección del aprendizaje automático

El aprendizaje automático avanzado ahora forma parte del motor de detección como una capa de protección avanzada, lo que mejora la detección. Lea lo siguiente antes de modificar un umbral (o nivel) de categoría

[Informar](#):

Cuando se detectan elementos

- **Sin acción:** no se realiza ninguna acción y el correo electrónico se entrega al destinatario
- **Mover a correo no deseado:** el correo electrónico se mueve a la carpeta correo no deseado.
- **Mover a la papelera:** el correo electrónico se mueve a la carpeta de la papelera.
- **Eliminar mensaje:** se elimina el correo electrónico.
- **Poner en cuarentena el mensaje:** el correo electrónico original se elimina y la copia del correo electrónico se almacena en cuarentena. Si decide liberar el correo electrónico de la cuarentena, se envía como un adjunto en un nuevo correo electrónico y se entrega al destinatario.
- **Eliminar archivo adjunto:** el archivo adjunto del mensaje se elimina y el mensaje se entrega al destinatario sin este.
- **Reemplazar adjunto:** el adjunto se reemplaza con un archivo de texto que contiene información detallada sobre una acción tomada.
- **Colocar el archivo adjunto en cuarentena:** el archivo adjunto se elimina del correo electrónico y se pone en cuarentena

Texto de sustitución de archivo adjunto

Reemplazar el adjunto con un archivo de texto que contiene información detallada sobre una acción tomada.

Asunto de la etiqueta

Cuando esté habilitado, puede modificar plantillas añadidas al asunto de mensajes infectados.

Texto de asunto de etiqueta

Puede agregar una etiqueta personalizada a los asuntos de los mensajes afectados.

Notificar al propietario del buzón

Cuando esta opción está habilitada, el usuario recibe un correo electrónico de notificación cuando se realiza una detección.

Idioma

Elija el idioma que desee en el menú desplegable. El propietario del buzón recibirá correos electrónicos de notificación en el idioma seleccionado cuando se libera un objeto de la cuarentena. Esta opción anula el idioma predeterminado del inquilino en la [configuración](#).

Notificar al administrador

Se especifica una dirección de correo electrónico (presionar Intro para agregar varias direcciones) que recibirá correos electrónicos de notificación siempre que se realice una detección.

[^ Protección contra spam de Gmail](#)

Habilitar protección contra spam de Gmail

Cuando está habilitada, esta función está activa y puede configurar opciones detalladas.

Cuando se detectan elementos

- **Sin acción:** no se realiza ninguna acción y el correo electrónico se entrega al destinatario
- **Mover a correo no deseado:** el correo electrónico se mueve a la carpeta correo no deseado.
- **Mover a la papelera:** el correo electrónico se mueve a la carpeta de la papelera.
- **Eliminar mensaje:** se elimina el correo electrónico.
- **Poner en cuarentena el mensaje:** el correo electrónico original se elimina y la copia del correo electrónico se almacena en cuarentena. Si decide liberar el correo electrónico de la cuarentena, se envía como un adjunto en un nuevo correo electrónico y se entrega al destinatario.

Asunto de la etiqueta

Cuando esté habilitado, puede modificar plantillas añadidas al asunto de mensajes infectados.

Texto de asunto de etiqueta

Puede agregar una etiqueta personalizada a los asuntos de los mensajes afectados.

Puede configurar listas de **Permitidos, Bloqueados e Ignorados** al especificar criterios como la dirección o el rango IP, el nombre del dominio, etc. Para agregar, modificar o eliminar criterios, haga clic en **Editar** para abrir la lista que desea administrar. De manera alternativa, puede importar su lista personalizada desde un archivo en lugar de agregar cada entrada de forma manual. Haga clic en **Importar** y busque el archivo (.txt) que contenga las entradas que desea agregar a la lista. Asimismo, si necesita exportar su lista actual a un archivo (.txt), seleccione **Exportar** desde el menú contextual.

Lista de IP aprobada	Coloca automáticamente en la lista blanca a los correos electrónicos que se originan desde direcciones IP especificadas. No se comprobará el contenido del correo electrónico.
Lista de IP bloqueada	Bloquea automáticamente los correos electrónicos que se originan desde direcciones IP especificadas.
Lista de IP ignorada	Lista de direcciones IP que se ignorarán durante la clasificación. Se comprobará el contenido del correo electrónico.
Lista de remitentes aprobados	Envía a la lista blanca los correos electrónicos que tienen su origen en un remitente o dominio específico. Para la verificación solo se utiliza una dirección de remitente o un dominio completo, en función de la siguiente prioridad: 1. Dirección SMTP "MAIL FROM" 2. Campo del encabezado de correo electrónico "Return-Path:" 3. Campo del encabezado de correo electrónico "X-Env-Sender:" 4. Campo del encabezado de correo electrónico "From:" 5. Campo del encabezado del correo electrónico "Sender:" 6. Campo del encabezado del correo electrónico "X-Apparently-From:"
Lista de remitentes bloqueados	Bloquea los correos electrónicos que tienen su origen en un remitente o dominio específico. Para la verificación se utilizan todas las direcciones de remitentes identificadas o todos los dominios: Dirección SMTP "MAIL FROM" Campo del encabezado de correo electrónico "Return-Path:" Campo del encabezado de correo electrónico "X-Env-Sender:" Campo del encabezado de correo electrónico "From:" Campo del encabezado del correo electrónico "Sender:" Campo del encabezado del correo electrónico "X-Apparently-From:"

 [Protección contra phishing de Gmail](#)

Habilitar Gmail Anti-Phishing

Cuando está habilitada, esta función está activa y puede configurar opciones detalladas.

Cuando se detectan elementos

- **Sin acción:** no se realiza ninguna acción y el correo electrónico con el adjunto malicioso se entrega al destinatario.
- **Mover a correo no deseado:** el correo electrónico se mueve a la carpeta correo no deseado.
- **Mover a la papelera:** el correo electrónico se mueve a la carpeta de la papelera.
- **Eliminar mensaje:** se elimina el correo electrónico.
- **Poner en cuarentena el mensaje:** el correo electrónico original se elimina y la copia del correo electrónico se almacena en cuarentena. Si decide liberar el correo electrónico de la cuarentena, se envía como un adjunto en un nuevo correo electrónico y se entrega al destinatario.

Asunto de la etiqueta

Cuando esté habilitado, puede modificar plantillas añadidas al asunto de mensajes infectados.

Texto de asunto de etiqueta

Puede agregar una etiqueta personalizada a los asuntos de los mensajes afectados.

Notificar al propietario del buzón

Cuando esta opción está habilitada, el usuario recibe un correo electrónico de notificación cuando se realiza una detección.

Notificar al administrador

Se especifica una dirección de correo electrónico (presionar Intro para agregar varias direcciones) que recibirá correos electrónicos de notificación siempre que se realice una detección.

Configuración de la protección para OneDrive

En esta sección, se aporta información sobre cómo cambiar las opciones y la configuración generales, de protección contra malware, contra spam o Anti-Phishing de OneDrive.

[Configuración general de OneDrive](#)

ESET LiveGrid® Comentarios sobre

Se enviarán datos al ESET Research Lab para su análisis posterior. Lea más sobre estas aplicaciones en el [glosario](#).

Registrar todos los objetos

Si se selecciona esta opción, todos los resultados de la exploración (incluidos los limpios) se mostrarán en [Registros de la exploración](#). La política de retención para los resultados de exploración de limpieza es de tres días. Los resultados de la exploración superiores a tres días se eliminarán de manera permanente.

[Protección contra malware de OneDrive](#)

Protección contra malware de OneDrive

Cuando está habilitada, esta función está activa y puede configurar opciones detalladas.

Informes y protección del aprendizaje automático

El aprendizaje automático avanzado ahora forma parte del motor de detección como una capa de protección avanzada, lo que mejora la detección. Lea lo siguiente antes de modificar un umbral (o nivel) de categoría

[Informar](#):

Cuando se detectan elementos

- **Sin acción:** no se realiza ninguna acción y el archivo permanece en OneDrive
- **Mover a la papelera de reciclaje:** el archivo se mueve a la papelera de reciclaje.
- **Reemplazar:** el contenido del archivo original se reemplaza por el texto que se indica a continuación en la ventana Texto de sustitución de archivo.
- **Cuarentena:** el archivo original se traslada a la papelera de reciclaje y se copia a cuarentena. Cuando se libera este archivo, el archivo eliminado previamente permanece en la papelera y se carga una nueva copia a la carpeta original de OneDrive.

Texto de sustitución de archivo

Reemplazar el adjunto con un archivo de texto que contiene información detallada sobre una acción tomada.

Notificar al propietario

Cuando esta opción está habilitada, el usuario recibe un correo electrónico de notificación cuando se realiza una detección.

Notificar al administrador

Se especifica una dirección de correo electrónico (presionar Intro para agregar varias direcciones) que recibirá correos electrónicos de notificación siempre que se realice una detección.

Configuración de la protección para Google Drive

En esta sección, se aporta información sobre cómo cambiar las opciones y la configuración generales, de protección contra malware, contra spam o Anti-Phishing de Google Drive.

[General de Google Drive](#)

ESET LiveGrid® Comentarios sobre

Se enviarán datos al ESET Research Lab para su análisis posterior. Lea más sobre estas aplicaciones en el [glosario](#).

Registrar todos los objetos

Si se selecciona esta opción, todos los resultados de la exploración (incluidos los limpios) se mostrarán en [Registros de la exploración](#). La política de retención para los resultados de exploración de limpieza es de tres días. Los resultados de la exploración superiores a tres días se eliminarán de manera permanente.

[Protección contra malware de Google Drive](#)

Protección contra malware de Google Drive

Cuando está habilitada, esta función está activa y puede configurar opciones detalladas.

Informes y protección del aprendizaje automático

El aprendizaje automático avanzado ahora forma parte del motor de detección como una capa de protección avanzada, lo que mejora la detección. Lea lo siguiente antes de modificar un umbral (o nivel) de categoría

[Informar](#):

Cuando se detectan elementos

- **Sin acción:** no se realiza ninguna acción y el archivo permanece en Google Drive
- **Mover a la papelera de reciclaje:** el archivo se mueve a la papelera de reciclaje.
- **Reemplazar:** el contenido del archivo original se reemplaza por el texto que se indica a continuación en la ventana Texto de sustitución de archivo.
- **Cuarentena:** el archivo original se traslada a la papelera de reciclaje y se copia a cuarentena.
- **Eliminar:** el archivo original se elimina permanentemente de Google Drive.

Texto de sustitución de archivo

Reemplazar el adjunto con un archivo de texto que contiene información detallada sobre una acción tomada.

Notificar al propietario

Cuando esta opción está habilitada, el usuario recibe un correo electrónico de notificación cuando se realiza una detección.

Notificar al administrador

Se especifica una dirección de correo electrónico (presionar Intro para agregar varias direcciones) que recibirá correos electrónicos de notificación siempre que se realice una detección.

Configuración de la protección para grupos del equipo

En esta sección, se aporta información sobre cómo cambiar las opciones y la configuración generales o de protección contra malware de los grupos del equipo.

[Configuración general de grupos del equipo](#)

ESET LiveGrid® Comentarios sobre

Se enviarán datos al ESET Research Lab para su análisis posterior. Lea más información sobre estos tipos de aplicaciones en el [glosario](#).

Registrar todos los objetos

Si se selecciona esta opción, todos los resultados de la exploración (incluidos los limpios) se mostrarán en [Registros de la exploración](#). La política de conservación para los resultados limpios de la exploración es de tres días. Los resultados de la exploración superiores a tres días se eliminarán de manera permanente.

[Protección contra malware de grupos del equipo](#)

Protección contra malware de grupos del equipo

Cuando está habilitada, esta función está activa y puede configurar opciones detalladas.

Informes y protección del aprendizaje automático

El aprendizaje automático avanzado ahora forma parte del motor de detección como una capa de protección avanzada, lo que mejora la detección. Lea lo siguiente antes de modificar un umbral (o nivel) de categoría

[Informar](#):

Cuando se detectan elementos

- **Sin acción:** no se realiza ninguna acción, el archivo permanece intacto.
- **Mover a la papelera de reciclaje:** el archivo se mueve a la papelera de reciclaje de Team.
- **Reemplazar:** el contenido del archivo original se sustituye por el texto que se indica a continuación en la ventana "texto de sustitución de archivo"
- **Cuarentena:** el archivo original se mueve a la papelera de reciclaje de Team y se copia en cuarentena. Cuando se libera este archivo, el archivo eliminado previamente permanece en la papelera y se carga una nueva copia a la ubicación original.

Texto de sustitución de archivo

Reemplazar el adjunto con un archivo de texto que contiene información detallada sobre una acción tomada.

Notificar al propietario

Cuando esta opción está habilitada, el usuario recibe un correo electrónico de notificación cuando se realiza una detección.

Notificar al administrador

Se especifica una dirección de correo electrónico (presionar Intro para agregar varias direcciones) que recibirá correos electrónicos de notificación siempre que se realice una detección.

Configuración de la protección para sitios de SharePoint

En esta sección, se aporta información sobre cómo cambiar las opciones y la configuración generales o de protección contra malware de los sitios de Sharepoint.

[^ Configuración general de Sitios de SharePoint](#)

ESET LiveGrid® Comentarios sobre

Se enviarán datos al ESET Research Lab para su análisis posterior. Lea más información sobre estos tipos de aplicaciones en el [glosario](#).

Registrar todos los objetos

Si se selecciona esta opción, todos los resultados de la exploración (incluidos los limpios) se mostrarán en [Registros de la exploración](#). La política de conservación para los resultados limpios de la exploración es de tres días. Los resultados de la exploración superiores a tres días se eliminarán de manera permanente.

[^ Protección contra malware de sitios de Sharepoint](#)

Protección contra malware de sitios de Sharepoint

Cuando está habilitada, esta función está activa y puede configurar opciones detalladas.

Informes y protección del aprendizaje automático

El aprendizaje automático avanzado ahora forma parte del motor de detección como una capa de protección avanzada, lo que mejora la detección. Lea lo siguiente antes de modificar un umbral (o nivel) de categoría

[Informar](#):

Cuando se detectan elementos

- **Sin acción:** no se realiza ninguna acción, el archivo permanece intacto.
- **Mover a la papelera de reciclaje:** el archivo se mueve a la papelera de reciclaje de SharePoint.
- **Reemplazar:** el contenido del archivo original se sustituye por el texto que se indica a continuación en la ventana "texto de sustitución de archivo"
- **Cuarentena:** el archivo original se mueve a la papelera de reciclaje de SharePoint y se copia en cuarentena.

Cuando se libera este archivo, el archivo eliminado previamente permanece en la papelera y se carga una nueva copia a la ubicación original.

Texto de sustitución de archivo

Reemplazar el adjunto con un archivo de texto que contiene información detallada sobre una acción tomada.

Notificar al propietario

Cuando esta opción está habilitada, el usuario recibe un correo electrónico de notificación cuando se realiza una detección.

Notificar al administrador

Se especifica una dirección de correo electrónico (presionar Intro para agregar varias direcciones) que recibirá correos electrónicos de notificación toda vez que se realice una detección.

Configuración de la protección de ESET LiveGuard

Advanced

Para usar la función ESET LiveGuard Advanced, configure una política que habilite el análisis por parte de ESET LiveGuard Advanced. Los usuarios o grupos asignados a esta política tendrán protección adicional. Los archivos enviados para el análisis por parte de ESET LiveGuard Advanced se muestran en la pestaña Archivos enviados; esto se aplica a muestras sospechosas desconocidas (nunca vistas). Los archivos maliciosos conocidos (basados en hash) no se envían para su análisis en ESET LiveGuard Advanced.

Verá los resultados de ESET LiveGuard Advanced en los [Registros de la exploración](#) (Exchange Online, OneDrive, grupos del equipo o sitios de SharePoint) marcados como  malware.

ESET LiveGuard Advanced

Cuando está habilitada, esta función está activa y puede configurar opciones detalladas.

 ESET LiveGuard Advanced habilitará automáticamente los comentarios de ESET LiveGrid®. Se enviarán datos al ESET Research Lab para su análisis posterior. Puede obtener más información sobre ESET LiveGrid® en el [glosario](#).

Límite de detección

Los resultados con un nivel de umbral seleccionado, y superiores, se considerarán amenazas.

Envío automático de muestras sospechosas (menú desplegable)

Este ajuste está relacionado con ESET LiveGrid® y permite las siguientes acciones: Todo, Todo excepto los documentos, Ninguno.

Envío automático de muestras sospechosas (barra deslizante)

Elija qué tipos de archivo se envían a ESET LiveGuard Advanced si contienen código sospechoso que, por su comportamiento o características inusuales, parecen amenazas:

- **Ejecutables** – .exe, .dll, .sys
- **Archivos** – .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
- **Scripts** – .bat, .cmd, .hta, .js, .vbs, .js, .ps1
- **Otro** – .jar, .reg, .msi, .swf, .lnk

Eliminar muestras sospechosas de los servidores de ESET

Elija cuándo eliminar las muestras que se enviaron para su análisis. Eliminar muestras de la nube de ESET LiveGuard Advanced: Nunca, Después de 30 días, Inmediatamente después del análisis.

Documentos

Use la barra deslizante para permitir el envío de documentos de Microsoft Office, PDF y otros tipos de documentos para el análisis por parte de ESET LiveGuard Advanced.

Borrar documentos desde servidores de ESET

Eliminar muestras de formato de archivos de documento de la nube de ESET LiveGuard Advanced: Nunca, Después de 30 días, Inmediatamente después del análisis.

Informes y protección del aprendizaje automático

El motor de detección brinda protección contra ataques maliciosos al sistema mediante la exploración de archivos, correos electrónicos y comunicación de redes. Si se detecta un objeto clasificado como malware, se inicia una corrección. El motor de detección puede eliminarlo al, en primer lugar, bloquearlo y, luego, iniciar algún tipo de acción, como limpiar, eliminar o mover a cuarentena.

Protección en tiempo real y con aprendizaje automático

El aprendizaje automático avanzado ahora forma parte del motor de detección como una capa de protección avanzada, lo que mejora la detección. Lea más sobre este tipo de protección en el [glosario](#) . Puede configurar los Niveles de informes para las siguientes categorías:

Malware

Un virus informático es un código malicioso que puede agregarse al principio o al final de archivos existentes en su equipo. Sin embargo, el término "virus" suele usarse en forma errónea. "Malware" (software malicioso) es un término más preciso. La detección de malware se realiza mediante la combinación del módulo del motor de detección con el componente de aprendizaje automático. Lea más información sobre estos tipos de aplicaciones en el [glosario](#) .

Aplicaciones potencialmente no deseadas (PUAs)

Una aplicación potencialmente no deseada es un software cuyo objetivo no es necesariamente malicioso. Sin

embargo, puede instalar software adicional no deseado, cambiar el comportamiento del dispositivo digital, realizar actividades que el usuario no aprueba o no espera, o tener otros objetivos no deseados. Esta categoría incluye: software de visualización de publicidad, descarga de envoltorios, distintas barras de herramientas de navegadores, software con comportamiento engañoso, bundleware, trackware. Lea más información sobre estos tipos de aplicaciones en el [glosario](#).

Aplicaciones potencialmente sospechosas

Es un software comprimido con [empaquetadores](#) o protectores frecuentemente usados para evitar la ingeniería inversa o para ofuscar el contenido de un ejecutable (por ejemplo, para ocultar la presencia de malware) mediante métodos propietarios de compresión o cifrado. Esta categoría incluye: todas las aplicaciones desconocidas comprimidas con empaquetadores o protectores utilizadas frecuentemente para comprimir malware.

Aplicaciones potencialmente no seguras

Esta clasificación se proporciona para el software comercial legítimo que pudiera usarse indebidamente con fines maliciosos. Una aplicación potencialmente no segura hace referencia al software comercial legítimo que se puede usar inadecuadamente para fines malintencionados. Esta categoría incluye: herramientas de descifrado, generadores de claves de licencia, herramientas de piratería informática, herramientas de control o acceso remoto, aplicaciones para adivinar contraseñas y los registradores de pulsaciones (programas que registran cada tecla pulsada por el usuario). Esta opción se encuentra deshabilitada en forma predeterminada. Lea más información sobre estos tipos de aplicaciones en el [glosario](#).

Informar

El motor de detección y el componente de aprendizaje automático se ocupan de realizar los informes. Puede definir el umbral de informes que mejor se adapte a su entorno y necesidades. No hay una única configuración correcta. Por lo tanto, le recomendamos que supervise el comportamiento dentro de su entorno y decida si hay otra configuración de informes más adecuada.

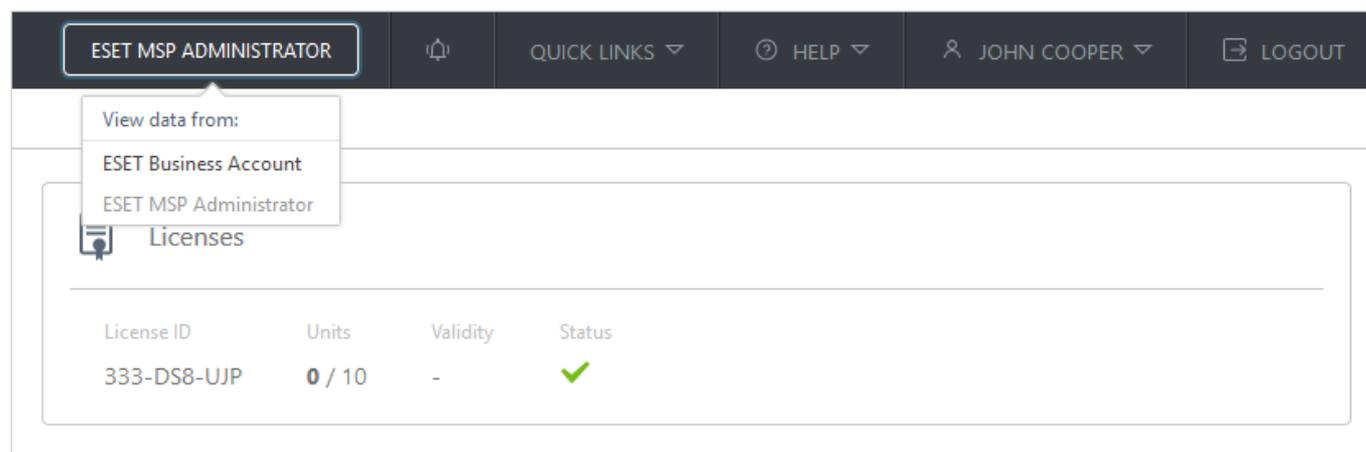
Los informes no ejercen ningún tipo de acción sobre los objetos. Ya que transmiten la información a una capa de protección correspondiente, y la capa de protección realiza las tareas pertinentes.

Intenso	Se han configurado los informes con máxima confidencialidad. Se informan más detecciones. Si bien el ajuste Intenso parecería ser el más seguro, a menudo también puede ser demasiado confidencial, lo que puede resultar contraproducente.  El ajuste Intenso puede identificar de manera falsa objetos como maliciosos y se iniciará una acción respecto de dichos objetos (según los ajustes de Protección).
Balanceado	Este ajuste es un equilibrio óptimo entre el rendimiento y la precisión de las tasas de detección y el número de objetos que se reportan falsamente.
Cauteloso	Informes que se configuran para minimizar la cantidad de objetos identificados en forma errónea al mismo tiempo que se mantiene un nivel suficiente de protección. Los objetos se informan únicamente cuando la probabilidad es evidente y concuerda con el comportamiento de un malware.
Desactivado	Informes no activos. No se hallaron, informaron ni limpiaron detecciones.  No pueden desactivarse los informes sobre malware. Por lo tanto, el ajuste Desactivado no se encuentra habilitado para el malware.

Administración de licencias

En la ventana principal, puede ver una descripción general de las licencias que se extraen, ESET Business Account o ESET MSP Administrator. Puede ver todos los grupos de licencias, sitios o empresas disponibles en el portal [ESET Business Account](#) o [ESET MSP Administrator](#). La administración de licencias le permite proteger o desproteger usuarios.

Si tiene la misma dirección de correo electrónico registrada en ESET MSP Administrator y ESET Business Account (inicio de sesión único), puede alternar entre las vistas ESET Business Account y ESET MSP Administrator (cuenta de licencias híbrida).



The screenshot shows the ESET license management interface. At the top, there is a dark navigation bar with the following elements: a button labeled 'ESET MSP ADMINISTRATOR', a notification bell icon, a 'QUICK LINKS' dropdown menu, a 'HELP' dropdown menu, a user profile 'JOHN COOPER' with a dropdown arrow, and a 'LOGOUT' button. Below the navigation bar, a dropdown menu is open, titled 'View data from:', with two options: 'ESET Business Account' and 'ESET MSP Administrator'. Below the dropdown, there is a section titled 'Licenses' with a table of license information.

License ID	Units	Validity	Status
333-DS8-UJP	0 / 10	-	✓

La licencia de ESET Cloud Office Security le permite usar la característica [ESET LiveGuard Advanced](#) sin cargo adicional. Verá la etiqueta ELG junto al ID de la licencia.

[Administración de licencias con ESET Business Account](#)

Muestra información sobre la licencia y el uso (nombre del grupo de licencias, identificación de licencias, unidades, validez y estado). Las licencias y los grupos de licencias se cargan desde ESET Business Account. Los [grupos de licencias](#) se encuentran disponibles únicamente si tiene [sitios existentes](#) en ESET Business Account (sitios útiles para la categorización). Una unidad representa la protección de ESET Cloud Office Security para un solo usuario de Exchange Online y OneDrive.

i Cada usuario protegido usa una unidad de licencia. Esto es independientemente de los servicios de Microsoft 365 que se usen. Un usuario con Exchange Online o OneDrive (o ambos) siempre consume una unidad de licencia. Ni los grupos del equipo ni los sitios de SharePoint usan una unidad de licencia.

Cada nuevo usuario aparecerá en la sección [Usuarios](#) como Desprotegido. Si usa la protección automática por inquilino o grupo, los nuevos usuarios se protegen de manera automática y se muestran como Protegidos.

Al proteger usuarios, tiene dos opciones:

- **Protección automática por inquilino o grupo (recomendado):** sin mantenimiento; se brinda protección de manera automática a todos los usuarios agregados recientemente que sean miembros de un grupo de Azure AD o que pertenezcan a un inquilino. Si desea obtener más información, consulte la siguiente nota.
- **Protección de usuario individual:** requiere administración y debe proteger manualmente a cada nuevo usuario.

Proteger a los usuarios (sin grupo de licencias)

1. Haga clic en **Proteger**.
2. Seleccione inquilino o grupo para la protección automática de los usuarios, y haga clic en **Proteger**. Para la protección de usuarios individuales, seleccione los usuarios que desea proteger y haga clic en **Proteger**. La política predeterminada ahora protege a los usuarios.
3. De ser necesario, especifique una política personalizada para los usuarios en la sección [Políticas](#).

Proteger a los usuarios (con un grupo de licencias)

1. Seleccione el grupo de licencias y haga clic en el icono de tres puntos  > **Mostrar detalles** junto al grupo de licencias.
2. Haga clic en **Proteger**.
3. Seleccione inquilino o grupo para la protección automática de los usuarios, y haga clic en **Proteger**. Para la protección de usuarios individuales, seleccione los usuarios que desea proteger y haga clic en **Proteger**. La política predeterminada ahora protege a los usuarios.
4. De ser necesario, especifique una política personalizada para los usuarios en la sección [Políticas](#).

i Asegúrese de tener suficientes unidades de licencia, especialmente con la protección automática habilitada cuando aumenta el número de usuarios. Cuando se usen todas las unidades de licencia, los nuevos usuarios que se conviertan en miembros de un inquilino o grupo no estarán protegidos. La protección de los usuarios existentes no se verá afectada. Si abre temporalmente las unidades de licencia y desea proteger a determinados usuarios, use grupos no protegidos (no use la protección automática) y proteja manualmente a los usuarios. Cuando aumente los grupos de licencias con más unidades, podrá volver a la protección automática para facilitar la administración.

Mover

Para mover usuarios entre grupos de licencias y para operaciones más avanzadas con licencias, haga clic para abrir [ESET Business Account](#).

Desproteger

1. Seleccione usuarios individuales, un inquilino o un grupo y haga clic en **Desproteger**.
2. Al eliminar la protección automática de un inquilino o grupo, se le preguntará si desea **Conservar protegidos a los usuarios de estos inquilinos o grupos**. Si decide no usar esta opción, los usuarios quedarán desprotegidos. Si marca la casilla de verificación, se desactivará la protección automática del grupo o inquilino, y se modificará por la protección de usuario individual. Los usuarios siguen estando protegidos, pero debe proteger manualmente a los usuarios recién agregados.


**Unprotect Tenants/Groups**
Do you want to unprotect selected tenants/groups?
 Keep users in these tenants/groups protected?
UNPROTECT **CANCEL**

Muestra información sobre la licencia y el uso (empresa del cliente, identificación de licencias, unidades y estado).

i Cada usuario protegido usa una unidad de licencia. Esto es independientemente de los servicios de Microsoft 365 que se usen. Un usuario con Exchange Online o OneDrive (o ambos) siempre consume una unidad de licencia.
Ni los grupos del equipo ni los sitios de SharePoint usan una unidad de licencia.

Cada nuevo usuario aparecerá en la sección [Usuarios](#) como **Desprotegido**. Si usa la protección automática por inquilino o grupo, los nuevos usuarios se protegen de manera automática y se muestran como **Protegidos**.

Al proteger usuarios, tiene dos opciones:

- **Protección automática por inquilino o grupo (recomendado)**: sin mantenimiento; se brinda protección de manera automática a todos los usuarios agregados recientemente que sean miembros de un grupo de Azure AD o que pertenezcan a un inquilino. Si desea obtener más información, consulte la siguiente nota.
- **Protección de usuario individual**: requiere administración y deberá proteger manualmente a cada nuevo usuario.

Proteger a los usuarios

1. Haga clic en **Proteger**.
2. Seleccione inquilino o grupo para la protección automática de los usuarios, y haga clic en **Proteger**. Para la protección de usuarios individuales, seleccione los usuarios que desea proteger y haga clic en **Proteger**. La política predeterminada ahora protege a los usuarios.
3. De ser necesario, especifique una política personalizada para los usuarios en la sección [Políticas](#).

i Asegúrese de tener suficientes unidades de licencia, especialmente con la protección automática habilitada cuando aumenta el número de usuarios. Cuando se usen todas las unidades de licencia, los nuevos usuarios que se conviertan en miembros de un inquilino o grupo no estarán protegidos. La protección de los usuarios existentes no se verá afectada.
Si abre temporalmente las unidades de licencia y desea proteger a determinados usuarios, use grupos no protegidos (no use la protección automática) y proteja manualmente a los usuarios. Cuando aumente los grupos de licencias con más unidades, podrá volver a la protección automática para facilitar la administración.

Desproteger

1. Seleccione usuarios individuales, un inquilino o un grupo y haga clic en **Desproteger**.
2. Al eliminar la protección automática de un inquilino o grupo, se le preguntará si desea **Conservar protegidos a los usuarios de estos inquilinos o grupos**. Si decide no usar esta opción, los usuarios quedarán desprotegidos. Si marca la casilla de verificación, se desactivará la protección automática del grupo o inquilino, y se modificará por la protección de usuario individual. Los usuarios siguen estando protegidos, pero debe proteger manualmente a los usuarios recién agregados.

Acceso de usuario de ESET Cloud Office Security a una empresa concreta

En un entorno con varios inquilinos, puede proporcionarle a un usuario acceso a ESET Cloud Office Security para permitir que este solo vea una empresa específica (con permiso de lectura o escritura). Esto suelen usarlo los proveedores de servicios gestionados.

Configure los derechos de acceso de un usuario en [ESET MSP Administrator](#) mediante la asignación de una empresa con permiso de **escritura** y acceso de **escritura** a ESET Cloud Office Security:

1. Inicie sesión en [ESET MSP Administrator](#) como administrador.
2. Edite un usuario y configure los **derechos de acceso a las empresas** bajo la opción Permisos y seleccione acceso de **escritura**. El usuario solo puede ver la empresa asignada con su grupo de licencias.

3. Establezca el acceso de **escritura** a ESET Cloud Office Security para que el usuario pueda proteger una empresa al agregar un inquilino. Un usuario con acceso de lectura no puede agregar ni quitar un inquilino.

The screenshot shows the 'Edit user' interface in ESET MSP Administrator. The left sidebar contains navigation options like DASHBOARD, LICENSE MANAGEMENT, COMPANIES, REPORTS, and User management. The main content area is titled 'Edit user' and has a 'PERMISSIONS' section. Under 'ACCESS RIGHTS', there are three radio button options: 'Write access to MSP [redacted] and all customers', 'Read access to MSP [redacted] and all customers', and 'No access to MSP [redacted] and custom access on customers'. Below this is a table for 'ACCESS RIGHTS TO COMPANIES' with columns for NAME, ACCESS, TYPE, and TAGS. The table lists 'plant' with 'Write' access and 'test1' with 'Read' access. At the bottom, there are buttons for 'SAVE', 'CANCEL', and 'DELETE USER'.

Solo se puede configurar un tipo de acceso a ESET Cloud Office Security como ajuste global y se aplica a todas las empresas (si a un usuario se le asignan varias empresas).

Registro de auditoría

Realiza un seguimiento de los cambios de configuración o protección de ESET Cloud Office Security. Los historiales del registro de auditoría demuestran las actividades y muestran la secuencia en la que se produjeron. Los registros de auditoría almacenan información sobre la operación o el suceso específicos. Los registros de auditoría se crean siempre que se crea o modifica un objeto de ESET Cloud Office Security (grupo de licencias, usuario, política, informe, elemento de cuarentena, como archivo adjunto).

Cuando hace clic en el ícono del engranaje  situado en la esquina superior derecha para acceder al menú contextual **Exportar a CSV**, puede exportar la tabla a formato CSV y utilizarla en otras aplicaciones para trabajar con la lista.

Haga clic en el ícono  para abrir una barra lateral con un resumen de un Registro de auditoría específico. Para obtener información más detallada, haga clic en el ícono  y seleccione **Mostrar detalles**.

Mosaico	Detalle
Información básica	Muestra los datos generales del registro de auditoría (Ocurrió, Acción, Gravedad, Resultado, Sección).

Mosaico	Detalle
Usuario	Muestra la información sobre el usuario que ejecutó una acción o realizó un cambio, incluido el correo electrónico y la dirección IP del usuario.
Cambios	Detalles de los cambios realizados.
Configuración anterior	Muestra la configuración anterior de políticas.
Nueva configuración	Muestra la configuración actual de políticas.
Objetos	Muestra los objetos afectados por el cambio o la acción (usuario, política, archivo adjunto, etc.).

Puede filtrar los usuarios usando varios criterios. Haga clic en **Agregar filtro** y seleccione un tipo de filtro del menú desplegable o introduzca una secuencia (se repite al combinar varios criterios):

Agregar filtro	Uso
Acción	Seleccione una de las acciones disponibles.
Objeto	Escriba un nombre de objeto válido.
Estado	Seleccione una de las siguientes opciones: Correcta, Fallida, Iniciada o Parcialmente correcta
Usuario	Escriba el usuario que realizó los cambios.
Gravedad	Seleccione el nivel de gravedad: Baja, Mediana o Alta
Ocurrió desde/Ocurrió hasta	Filtrado por hora del suceso. Use Ocurrió desde y haga clic en la fecha para mostrar solo los registros más recientes de la fecha especificada. Use Ocurrió para los registros anteriores o use ambos para el intervalo de tiempo deseado.
Se ha iniciado el sistema	Filtra los registros realizados por el sistema.

Enviar comentarios

Para enviar sus comentarios en la consola de ESET Cloud Office Security, use la barra de herramientas de la esquina superior derecha, coloque el cursor del mouse sobre **Ayuda** y haga clic en **Enviar comentarios**. Elija **Díganos lo que piensa** (compartir ideas y experiencias) o **Informar de un problema o fallo**.

Soporte técnico

Utilice los siguientes enlaces que incluyen información de soporte que lo ayudarán a resolver los problemas que puedan surgir:

Buscar en la base de conocimientos de ESET

La [base de conocimiento de ESET](#) contiene respuestas a las preguntas más frecuentes y soluciones recomendadas para varios problemas. La actualización regular por parte de los especialistas técnicos de ESET convierte a la base de conocimiento en la herramienta más potente para resolver varios tipos de problemas.

Visitar el foro de ESET Security

[Foro de soporte](#) El foro de ESET proporciona a los usuarios de ESET una manera fácil de obtener ayuda y ayudar a otros. Puede publicar cualquier problema o pregunta relacionados con sus productos ESET.

Comuníquese con el Soporte técnico

[Formulario de soporte técnico de ESET](#) Complete el formulario para proporcionar sus datos, incluida la descripción del problema.

Comuníquese con su socio local de ESET para obtener ayuda

[Comuníquese con su soporte local de ESET](#) Localice la información de contacto de soporte del equipo de soporte de ESET de su región en el correo electrónico de su licencia de ESET.

Enviar comentarios

[Enviar comentarios](#) Díganos lo que piensa (comparta ideas y experiencias) o informe de un problema o fallo.

Sugerir mejoras para la ayuda en línea

Puede publicar su calificación y proporcionar comentarios sobre un tema específico de ayuda en línea haciendo clic en el enlace **¿Le resultó útil la información?** debajo de la página de ayuda. Háganos saber si el contenido le sirvió de ayuda o cómo cree que nuestro escritor técnico podría mejorarlo.

Disponibilidad del servicio

El [Portal de estado de ESET](#) muestra el estado actual de los servicios en la nube de ESET, las interrupciones programadas y los incidentes pasados. Si tiene un problema con un servicio ESET compatible y no lo ve mencionado en el Portal de estado, comuníquese con [Soporte técnico de ESET](#).

Los equipos de monitoreo verifican los posibles problemas internamente, y los incidentes confirmados se publican y actualizan manualmente para mantener la credibilidad y precisión. Por lo tanto, aparecen en el Portal de estado con un ligero retraso. Es posible que no publiquemos incidentes breves si se resuelven antes de confirmarlos manualmente.

Security for ESET Cloud Office Security

Introducción

La finalidad de este documento es resumir las prácticas de seguridad y los controles de seguridad que se aplican en ESET Cloud Office Security. Las prácticas y los controles de seguridad están diseñados para proteger la confidencialidad, la integridad y la disponibilidad de la información del cliente. Tenga en cuenta que las prácticas y los controles de seguridad pueden cambiar.

Alcance

El alcance de este documento es resumir las prácticas y controles de seguridad de infraestructura de ESET Cloud Office Security, ESET Business Account (en adelante, "EBA"), ESET Data Framework, ESET LiveGrid, actualización, antispam, infraestructura de ESET Dynamic Threat Defense, organización, personal y procesos operativos. Entre las prácticas y controles de seguridad se incluyen:

1. Políticas de seguridad de la información
2. Organización de la seguridad de la información

3. Seguridad de los recursos humanos
4. Administración de recursos
5. Control de acceso
6. Criptografía
7. Seguridad física y ambiental
8. Seguridad de operaciones
9. Seguridad de las comunicaciones
10. Adquisición, desarrollo y mantenimiento del sistema
11. Relación con el proveedor
12. Administración de incidentes de seguridad de la información
13. Aspectos de seguridad de la información de la administración de la continuidad empresarial
14. Cumplimiento

Concepto de seguridad

La empresa ESET s.r.o. cuenta con la certificación ISO 27001:2013 con un alcance integrado en el sistema de administración, que abarca explícitamente ESET Cloud Office Security, EBA y otros servicios.

Por lo tanto, el concepto de seguridad de la información usa el marco de la norma ISO 27001 con el fin de implementar una estrategia de seguridad de defensa escalonada al momento de aplicar los controles de seguridad en la capa de la red, sistemas operativos, bases de datos, aplicaciones, personal y procesos operativos. Las prácticas y controles de seguridad aplicados tienen por objetivo superponerse y complementarse entre sí.

Prácticas y controles de seguridad

1. Políticas de seguridad de la información

ESET usa políticas de seguridad de la información para abarcar todos los aspectos de la norma ISO 27001, incluidos los controles y prácticas de seguridad, y la gestión de seguridad de la información. Las políticas se revisan de forma anual y se actualizan tras cambios importantes para garantizar su idoneidad, adecuación y eficacia continuas.

ESET realiza revisiones anuales de esta política y de comprobaciones de seguridad internas para garantizar la coherencia con esta política. El incumplimiento de las políticas de seguridad de la información está sujeto a medidas disciplinarias para los empleados de ESET o sanciones contractuales hasta la terminación del contrato para los proveedores.

2. Organización de la seguridad de la información

La organización de seguridad de la información de ESET Cloud Office Security consta de varios equipos e individuos implicados en la seguridad de la información y TI, lo que incluye:

- Administración ejecutiva de ESET
- Equipos de seguridad interna de ESET
- Equipos de TI de aplicaciones empresariales
- Otros elementos de apoyo

Las responsabilidades de seguridad de la información se asignan de acuerdo con las políticas de seguridad de la información implementadas. Los procesos internos se identifican y evalúan para determinar si existe cualquier riesgo de modificación no autorizada o no intencional, o un mal uso del producto de ESET. Las actividades riesgosas o delicadas de los procesos internos adoptan el principio de repartición de tareas para mitigar el riesgo.

El equipo jurídico de ESET es responsable de los contactos con las autoridades gubernamentales, incluidos los organismos reguladores eslovacos sobre seguridad informática y protección de datos personales. El equipo de seguridad interna de ESET es responsable de ponerse en contacto con grupos de interés especiales, como ISACA. El equipo del laboratorio de investigación de ESET es responsable de la comunicación con otras empresas de seguridad y la gran comunidad de seguridad informática.

La seguridad de la información se explica en la administración de proyectos con el marco de administración de proyectos aplicado, desde el proceso de concepción hasta la finalización del proyecto.

El trabajo remoto y el transporte se cubren mediante el uso de una política implementada en dispositivos móviles que incluye el uso de una potente protección de datos criptográficos en dispositivos móviles cuando se desplaza a través de redes no confiables. Los controles de seguridad de los dispositivos móviles están diseñados para funcionar de forma independiente de las redes internas de ESET y los sistemas internos.

3. Seguridad de los recursos humanos

ESET usa prácticas estándar de recursos humanos, incluidas políticas diseñadas para proteger la seguridad de la información. Estas prácticas abarcan todo el proceso de aprendizaje de empleados y se aplican a todos los empleados que acceden al entorno de ESET Cloud Office Security.

4. Administración de recursos

La infraestructura de ESET Cloud Office Security se incluye en los inventarios de recursos de ESET, con propiedad estricta y reglas aplicadas según el tipo de objeto y la sensibilidad. ESET tiene un esquema de clasificación interno definido. Todos los datos y configuraciones de ESET Cloud Office Security se clasifican como confidenciales.

5. Control de acceso

La política de control de acceso de ESET rige todos los accesos de ESET Cloud Office Security. El control de acceso se establece en la infraestructura, los servicios de red, el sistema operativo, la base de datos y el nivel de la aplicación. La administración del acceso completo a los usuarios a nivel de la aplicación es autónoma. El inicio de sesión único de ESET Cloud Office Security y ESET Business Account se rige por un proveedor de identidad central que garantiza que un usuario solo puede acceder al inquilino autorizado. La aplicación usa permisos de ESET Cloud Office Security estándar para aplicar control de acceso basado en roles para el inquilino.

El acceso al backend de ESET está limitado estrictamente a personas y roles autorizados. Los procesos estándar de ESET para el registro de usuarios (o la baja de registro), el aprovisionamiento (o su cancelación), la administración de privilegios y la revisión de los derechos de acceso de los usuarios se usan para administrar el acceso de los empleados de ESET a la infraestructura de ESET Cloud Office Security y las redes.

Existe una autenticación segura para proteger el acceso a todos los datos de ESET Cloud Office Security.

6. Criptografía

Para proteger los datos de ESET Cloud Office Security, se usa una potente criptografía para cifrar los datos en reposo y en tránsito. Por lo general, la autoridad certificadora de confianza se usa para emitir certificados para servicios públicos. La infraestructura de clave pública de ESET interna se usa para administrar las claves de la infraestructura de ESET Cloud Office Security. Los datos almacenados en la base de datos están protegidos por claves de cifrado generadas por la nube. Todos los datos de la copia de seguridad están protegidos por claves administradas de ESET.

7. Seguridad física y ambiental

Dado que ESET Cloud Office Security y ESET Business Account están basados en la nube, dependemos de Microsoft Azure para la seguridad física y ambiental. Microsoft Azure usa centros de datos certificados con medidas sólidas de seguridad física. La ubicación física del centro de datos depende de la selección de la región del cliente.

8. Seguridad de operaciones

El servicio de ESET Cloud Office Security se opera mediante medios automatizados basados en estrictos procedimientos operativos y plantillas de configuración. Todos los cambios, incluidos los cambios de configuración y la nueva implementación del paquete, se aprueban y probarán en un entorno de prueba específico antes de la instalación para la producción. Los entornos de desarrollo, prueba y producción se separan entre sí. Los datos de ESET Cloud Office Security solo se encuentran en el entorno de producción.

El entorno de ESET Cloud Office Security se supervisa con la supervisión operativa para identificar problemas rápidamente y proporcionar suficiente capacidad a todos los servicios de la red y los niveles de host.

Todos los datos de configuración se almacenan en nuestros repositorios de copias de seguridad periódicas para permitir la recuperación automática de la configuración de un entorno. Las copias de seguridad de los datos de ESET Cloud Office Security se almacenan tanto in situ como fuera del sitio.

Las copias de seguridad se cifran y prueban periódicamente para garantizar su recuperación como parte de las pruebas de continuidad empresarial.

La auditoría de los sistemas se realiza de acuerdo con las normas y las directrices internas. Los registros y eventos de la infraestructura, el sistema operativo, la base de datos, los servidores de aplicaciones y los controles de seguridad se recopilan continuamente. El equipo de TI y seguridad interna procesan aún más los registros para identificar anomalías operativas y de seguridad e incidentes de seguridad de la información.

ESET usa un proceso de administración general de vulnerabilidades técnicas para gestionar la aparición de vulnerabilidades en la infraestructura de ESET, incluido ESET Cloud Office Security y otros productos de ESET. Este proceso incluye exploración proactiva de vulnerabilidades y reiteradas pruebas de penetración de infraestructura, productos y aplicaciones.

ESET indica directrices internas para la seguridad de la infraestructura interna, las redes, los sistemas operativos, las bases de datos, los servidores de aplicaciones y las aplicaciones. Estas directrices se verifican mediante la supervisión del cumplimiento técnico y nuestro programa de auditoría de seguridad de la información interna.

9. Seguridad de las comunicaciones

El entorno de ESET Cloud Office Security se segmenta a través de la segmentación en la nube nativa, con acceso limitado a la red solo a los servicios necesarios entre los segmentos de red. La disponibilidad de los servicios de red se consigue mediante controles de nube nativa, como zonas de disponibilidad, equilibrio de carga y redundancia. Los componentes de equilibrio de carga especiales se implementan para proporcionar puntos de conexión específicos para el enrutamiento de instancias de ESET Cloud Office Security que aplican la autorización del tráfico y el equilibrio de carga. El tráfico de red se supervisa continuamente para detectar anomalías operativas y de seguridad. Los posibles ataques se pueden resolver con controles de nube nativa o soluciones de seguridad implementadas. Todas las comunicaciones de red se cifran a través de técnicas disponibles en general, incluidas IPsec y TLS.

10. Adquisición, desarrollo y mantenimiento del sistema

El desarrollo de los sistemas ESET Cloud Office Security se realiza de conformidad con la política de desarrollo de software seguro de ESET. Los equipos de seguridad interna se incluyen en el proyecto de desarrollo de ESET Cloud Office Security desde la fase inicial y supervisan todas las actividades de desarrollo y mantenimiento. El equipo de seguridad interna define y comprueba la ejecución de los requisitos de seguridad en varias etapas del desarrollo de software. La seguridad de todos los servicios, incluidos los recién desarrollados, se prueba continuamente tras su lanzamiento.

11. Relación con el proveedor

Las relaciones con proveedores relevantes se realizan de acuerdo con directrices válidas de ESET, que cubren toda la administración de las relaciones y los requisitos contractuales desde la perspectiva de la seguridad y la privacidad de la información. La calidad y seguridad de los servicios prestados por el proveedor de servicios críticos se evalúan periódicamente.

12. Administración de seguridad de la información

La administración de incidentes de seguridad de la información en ESET Cloud Office Security se realiza de forma similar a lo que se realiza en otras infraestructuras de ESET, y se basa en procedimientos de respuesta a incidentes definidos. Las funciones dentro de la respuesta a incidentes se definen y asignan a través de varios ámbitos, como el de TI, seguridad, derecho, recursos personales, relaciones públicas y administración ejecutiva. El equipo de respuesta a incidentes se establece en función de la clasificación de incidentes por parte del equipo de seguridad interno. Ese equipo brindará más información sobre el resto de equipos que gestionarán el incidente. El equipo de seguridad interno también es responsable de la recopilación de los conocimientos y las lecciones aprendidas. La ocurrencia y la resolución de los incidentes se comunican a las partes afectadas. El equipo jurídico de ESET es responsable de notificar a los organismos normativos si es necesario de acuerdo con el Reglamento General de Protección de Datos de la Unión Europea (GDPR) y la Ley de seguridad informática, que establece la Directiva de seguridad de la red y la información (NIS).

13. Aspectos de seguridad de la información de la administración de la continuidad empresarial

La continuidad empresarial del servicio de ESET Cloud Office Security se codifica en la arquitectura sólida usada para maximizar la disponibilidad de los servicios proporcionados. La restauración completa a partir de datos de copia de seguridad y configuración fuera del sitio es posible en caso de falla catastrófica de todos los nodos redundantes de los componentes ESET Cloud Office Security o el servicio ESET Cloud Office Security. El proceso de restauración se pone a prueba periódicamente.

14. Cumplimiento

El cumplimiento de los requisitos contractuales y regulatorios de ESET Cloud Office Security se evalúa y se revisa de manera periódica, al igual que otras infraestructuras y otros procesos de ESET. Además, se toman las medidas necesarias para garantizar el cumplimiento continuo. ESET está registrado como proveedor de servicios digitales para servicios digitales de informática en la nube que cubren varios servicios de ESET, incluido ESET Cloud Office Security. Tenga en cuenta que las actividades de cumplimiento de ESET no tienen por qué significar que los requisitos generales de cumplimiento de los clientes se cumplan como tales.

Términos de uso

Vigente a partir del 23 de octubre de 2023 | [Consulte una versión anterior de los Términos de uso](#) | [Comparar cambios](#)

Este acuerdo de ESET Cloud Office Security (en adelante denominado "Términos") constituye un acuerdo especial entre ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, inscrita en el Registro Mercantil administrado por el Tribunal de Distrito de Bratislava I, sección Sro, inscripción n.º 3586/B, número de registro mercantil: 31333532 (en adelante denominado "ESET" o "proveedor") y usted, persona física o jurídica (en adelante denominado "usted" o "usuario") que accede a una cuenta para administración, ESET Cloud Office Security y que accede al portal basado en la Web que controla ESET (en adelante denominado "Cuenta") para usar ESET Cloud Office Security. Si usa la cuenta y ESET Cloud Office Security (denominados, en adelante y en forma conjunta, el "Producto") en nombre de una organización, usted acepta estos términos para dicha organización y garantiza que tiene la autoridad para vincular a la organización con dichos Términos. En tal caso, los términos "usuario" y "usted" harán referencia a dicha organización. Lea estos Términos cuidadosamente, ya que se relacionan además con los servicios prestados por ESET o con el producto. Las condiciones específicas de uso de servicios individuales más allá de estos Términos están declarados con cada servicio, donde la aceptación formará parte del proceso de activación de servicio. Los anexos adjuntos sirven de complemento a estos Términos.

Seguridad y protección de datos

La cuenta brinda acceso a los servicios proporcionados por ESET. El nombre completo del usuario, el nombre de la compañía, país, dirección de correo electrónico válida, número de teléfono, datos de otorgamiento de licencia y estadísticas se requieren para el registro y el uso de la Cuenta y para la prestación y mantenimiento de servicios accedidos a través de Cuenta. Por la presente Usted acepta a que se recolecten y transfieran datos a los servidores del Proveedor o de sus socios. La única finalidad es garantizar la funcionalidad y la autorización de uso del Software, y la protección de los derechos del Proveedor. Tras la finalización de estos Términos, el Proveedor o cualquiera de sus socios tendrán el derecho a transferir, procesar y almacenar datos esenciales que identifiquen al Usuario por motivos de soporte y para la ejecución de estos Términos. Usted está autorizado a usar la Cuenta únicamente para los fines y en la manera establecida en virtud de estos Términos, términos de servicio individual y documentación.

Usted es responsable por mantener la seguridad de su Cuenta y la credenciales necesarias para el inicio de sesión. ESET no será responsable por pérdidas o daños derivados de su falta de cumplimiento con la obligación de mantener la seguridad. El Usuario además es responsable por cualquier actividad relacionada con el uso de la Cuenta, fuera o no autorizada. Si la Cuenta está comprometida, lo deberá notificar al Proveedor de inmediato.

Para proporcionar un servicio de administración de Cuenta, se requiere la recopilación de datos respecto de sus dispositivos administrados junto con la información de administración (en adelante, referido como "Datos"). Los Datos son proporcionados por Usted a ESET únicamente para la prestación del servicio de administración de Cuenta. Los Datos serán procesados y almacenados de conformidad con las políticas de seguridad y las prácticas de ESET y también con la Política de Privacidad.

Los detalles sobre la privacidad, protección de datos personales y derechos como el titular de datos se pueden encontrar en la [Política de Privacidad](#).

Política de uso justo

Usted tiene la obligación de cumplir con las limitaciones técnicas estipuladas en la documentación. Usted acepta que solamente usará el Software y sus funciones de una manera que no limite las posibilidades de otros Usuarios finales para acceder a estos servicios. El Proveedor se reserva el derecho de limitar el alcance los servicios proporcionados a Usuarios finales individuales, para activar el uso de los servicios por parte de la mayor cantidad posible de Usuarios finales. La limitación del alcance de los servicios también significará la finalización completa de la posibilidad del uso de cualquiera de las funciones de la Cuenta y eliminación de los datos e información.

En [Limitaciones](#) puede encontrar información detallada sobre las limitaciones técnicas.

Ubicación

El proveedor le podrá permitir elegir entre las ubicaciones del host disponibles para la Cuenta, incluso la ubicación recomendada elegida por el Proveedor. El Usuario reconoce que al elegir ubicaciones distintas a la recomendada, la experiencia de usuario puede verse afectada. En función de la ubicación elegida, se pueden aplicar el Acuerdo de Protección de datos incluido en el Anexo n.º 2 de este Acuerdo y las Cláusulas Contractuales Estándar incluidas en el Anexo n.º 3. ESET se reserva el derecho de cambiar la ubicación específica en cualquier momento, sin notificación previa, a los efectos de mejorar los servicios provistos por ESET de conformidad con Sus preferencias de ubicación (p. ej., Unión Europea).

Software

ESET o sus respectivos proveedores son propietarios o pueden ejercer derechos de autor sobre todo el software disponible como parte del Producto (en adelante, denominado "Software"). El Software se puede usar solo de acuerdo con el Acuerdo de licencia de usuario final incluido en el Anexo N.º 1 del presente Acuerdo. Otra información relacionada con el otorgamiento de licencias, copyright, documentación y marcas registradas está estipulada en en la [Información Legal](#).

Restricciones

No puede copiar, distribuir, extraer componentes o crear versiones derivadas del Software. Al usar la Cuenta, Usted tiene la obligación de cumplir con las siguientes restricciones:

- (a) No puede utilizar, modificar, traducir ni reproducir la Cuenta, o transferir los derechos del uso de la Cuenta o sus componentes de ninguna otra forma a lo establecido en estos Términos.
- (b) No puede vender, sublicenciar, arrendar o alquilar la Cuenta, ni usarla para suministrar servicios comerciales.
- (c) No puede aplicar técnicas de ingeniería inversa, descompilar o desmontar la Cuenta, ni intentar obtener el código fuente de la Cuenta de ninguna otra forma, salvo en la medida en que esta restricción esté explícitamente prohibida por la ley.
- (d) Usted acepta que solo usará la Cuenta de conformidad con todas las leyes aplicables en la jurisdicción en la que lo utilice, incluidas, a mero título enunciativo, las restricciones aplicables relacionadas con el copyright y otros derechos de propiedad intelectual.

Declaraciones del Usuario Final

COMO USUARIO, RECONOCE POR LA PRESENTE QUE LA CUENTA Y LOS SERVICIOS SE OFRECEN "TAL CUAL", SIN GARANTÍA DE NINGÚN TIPO, NI EXPLÍCITA NI IMPLÍCITA, EN LA MEDIDA QUE LO PERMITA LA LEGISLACIÓN APLICABLE. NI EL PROVEEDOR, NI SUS LICENCIADORES O FILIALES, NI LOS TITULARES DE LOS DERECHOS DE AUTOR OFRECEN NINGUNA GARANTÍA O DECLARACIÓN, NI EXPLÍCITA NI IMPLÍCITA, LO QUE INCLUYE, ENTRE OTRAS COSAS, LAS GARANTÍAS DE COMERCIALIZACIÓN O ADECUACIÓN A UN PROPÓSITO ESPECÍFICO O QUE LA CUENTA O LOS SERVICIOS INFRINJAN LAS PATENTES, LOS DERECHOS DE AUTOR, LAS MARCAS U OTROS DERECHOS DE TERCEROS. NI EL PROVEEDOR NI NINGUNA OTRA PARTE GARANTIZAN QUE LA CUENTA O LOS SERVICIOS CUMPLIRÁN SUS REQUISITOS NI QUE EL FUNCIONAMIENTO DE LA CUENTA O DE LOS SERVICIOS SUFRA INTERRUPCIONES NI ERRORES. USTED ASUME TODOS LOS RIESGOS Y RESPONSABILIDAD DE LA SELECCIÓN Y EL USO DE LA CUENTA Y LOS SERVICIOS PARA CONSEGUIR LOS RESULTADOS QUE DESEA Y POR LOS RESULTADOS OBTENIDOS.

Este Acuerdo no crea obligaciones del lado del Proveedor y sus licenciatarios, excepto las obligaciones

específicamente indicadas en este Acuerdo.

Limitación de responsabilidad

EN LA MEDIDA EN QUE LO PERMITA LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O COLABORADORES SERÁN RESPONSABLES DE PÉRDIDAS DE INGRESOS, GANANCIAS, VENTAS, DATOS O COSTOS DE ADQUISICIÓN DE BIENES O SERVICIOS SUSTITUIDOS, DAÑOS A LA PROPIEDAD, DAÑOS PERSONALES, INTERRUPCIÓN DEL NEGOCIO, PÉRDIDA DE INFORMACIÓN COMERCIAL O DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, ACCIDENTALES, ECONÓMICOS, DE COBERTURA, DAÑOS PUNITIVOS, ESPECIALES O CONSECUENCIALES, MÁS ALLÁ DE QUE SEAN PROVOCADOS O DERIVADOS DEL CONTRATO, AGRAVIO, NEGLIGENCIA O CUALQUIER OTRA TEORÍA DE RESPONSABILIDAD, QUE SE DERIVEN DEL USO O LA INCAPACIDAD DE USAR LA CUENTA, AUNQUE EL PROVEEDOR, SUS PROVEEDORES DE INFORMACIÓN Y AFILIADOS RECIBAN INFORMACIÓN DE LA POSIBILIDAD DE DICHS DAÑOS. ALGUNOS PAÍSES Y JURISDICIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR SU LIMITACIÓN, POR LO QUE, EN DICHS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR Y SUS EMPLEADOS, PROVEEDORES DE SERVICIOS O AFILIADOS SE LIMITA A LA SUMA QUE PAGÓ POR EL SERVICIO O LA CUENTA EN CUESTIÓN.

Cumplimiento del control comercial

(a) Usted no podrá, ya sea directa o indirectamente, exportar, reexportar o transferir el Software, o de alguna otra forma ponerlo a disposición de ninguna persona, o utilizarlo de ninguna manera, o participar de ningún acto, que pueda ocasionar que ESET o sus compañías controladoras, sus empresas subsidiarias y las subsidiarias de cualquiera de sus compañías controladoras, así como también las entidades controladas por sus compañías controladoras ("Afiliadas") violen, o queden sujetas a las consecuencias negativas de las Leyes de Control Comercial, las cuales incluyen:

i. todas las leyes que controlen, restrinjan o impongan requisitos de licencia sobre la exportación, la reexportación o la transferencia de bienes, software, tecnología o servicios, emitidas o aprobadas por cualquier autoridad gubernamental, estado o normativa de los Estados Unidos de América, Singapur, Reino Unido, la Unión Europea o cualquiera de sus Estados miembro, o cualquier país en el que deban cumplirse las obligaciones establecidas en estos Términos, o en el que ESET o cualquiera de sus Filiales se encuentran incorporadas u operan; y

ii. todas las medidas económicas, financieras, comerciales u otras, sanciones, restricciones, embargos, prohibición de importación o exportación, prohibición de transferencia de fondos o recursos o prestación de servicios, o medidas equivalentes impuestas por cualquier autoridad gubernamental, estatal o regulatoria de los Estados Unidos de América, Singapur, Reino Unido, la Unión Europea o cualquiera de sus Estados miembro, o cualquier país en el que deban cumplirse las obligaciones establecidas en estos Términos, o en el que ESET o cualquiera de sus Filiales se encuentran incorporadas u operan (actos legales mencionados en los puntos i y ii. Anteriormente denominados "Leyes de control comercial").

(b) ESET tendrá el derecho de suspender sus obligaciones conforme a estos Términos o terminar el Acuerdo, con efecto inmediato, en los siguientes casos:

i. ESET determina que, en su razonable opinión, el Usuario ha violado o podría violar la disposición de la Sección (a) de esta cláusula de Cumplimiento del control comercial de estos Términos; o

ii. el Usuario final o el Software quedan sujetos a las Leyes de Control Comercial y, en consecuencia, ESET determina que, en su razonable opinión, el cumplimiento continuo de sus obligaciones conforme a los Términos podría ocasionar que ESET o sus Afiliadas incurriesen en la violación de las Leyes de Control Comercial o quedasen sujetas a las consecuencias negativas de estas.

(c) Ninguna de las estipulaciones de los Términos tiene por objeto inducir o exigir, ni debe interpretarse como una

intención de inducir o exigir a ninguna de las partes actuar o abstenerse de actuar (o acordar actuar o abstenerse de actuar) de ninguna manera que resulte inconsistente con las Leyes de Control Comercial aplicables, o se encuentre penalizada o prohibida por estas.

Ley vigente e idioma

Estos Términos se regirán e interpretarán de acuerdo con la legislación eslovaca. El Usuario final y el Proveedor aceptan que las disposiciones ante conflictos de la legislación vigente y la Convención de las Naciones Unidas sobre los Contratos de Venta Internacional de Bienes no serán aplicables. Si es un consumidor con domicilio habitual en la UE, también se le concede protección adicional mediante disposiciones legales obligatorias aplicables en su país de origen.

Acepta expresamente que la jurisdicción exclusiva en caso de reclamaciones o disputas con el Proveedor o relacionadas de cualquier forma con su uso del Software, la Cuenta o los Servicios, o que se deriven de estos Términos o Términos especiales (si corresponde), corresponde al Tribunal de Distrito de Bratislava I (Eslovaquia), y además acepta explícitamente el ejercicio de la jurisdicción personal en el Tribunal de Distrito de Bratislava I en relación con dichas reclamaciones o disputas. Si es un consumidor y tiene un domicilio habitual en la UE, también puede presentar una reclamación para exigir sus derechos de consumidor en el lugar de la jurisdicción exclusiva o en el país de la UE en el que vive. También puede usar una plataforma de resolución de controversias en línea, a la que se puede acceder aquí: <https://ec.europa.eu/consumers/odr/>. No obstante, puede ponerse en contacto con nosotros en primer lugar antes de realizar cualquier reclamación de forma oficial.

Si existen discrepancias entre las versiones en diferentes idiomas de estos Términos, siempre prevalecerá la versión en inglés disponible [aquí](#).

Disposiciones generales

ESET se reserva el derecho de revisar estos Términos y la documentación, o cualquier parte de ellos, en cualquier momento sin previo aviso mediante la actualización de la documentación relevante para reflejar los cambios en la legislación o en la Cuenta. Se le notificará cualquier revisión de estos Términos mediante el Software. Si no está de acuerdo con los cambios de estos Términos, podrá cancelar la Cuenta. A menos que cancele su Cuenta luego de recibir una notificación en relación con los cambios, estará obligado por las modificaciones o revisiones de estos Términos. Se le recomienda visitar esta página periódicamente para revisar los TDS que aplican actualmente a su uso de la Cuenta.

Avisos

Todos los avisos deben entregarse a: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

Anexo N.º 1

[Acuerdo de Licencia de Usuario Final](#)

Anexo n.º 2

[Contrato de procesamiento de datos](#)

Anexo n.º 3

[Disposiciones contractuales estándar](#)

Acuerdo de licencia de usuario final

IMPORTANTE: Lea los términos y las condiciones del producto de aplicación que se especifican abajo antes de descargarlo, instalarlo, copiarlo o usarlo. **AL DESCARGAR, INSTALAR, COPIAR O UTILIZAR EL SOFTWARE, USTED DECLARA SU CONSENTIMIENTO CON LOS TÉRMINOS Y CONDICIONES Y RECONOCE QUE HA LEÍDO LA [POLÍTICA DE PRIVACIDAD](#).**

Acuerdo de Licencia de Usuario Final

Bajo los términos de este Acuerdo de licencia de usuario final (en adelante, el "Acuerdo") celebrado entre ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, Slovak Republic, inscrita en el Registro Mercantil y de Sociedades administrado por el Tribunal del Distrito I de Bratislava, Sección Sro, Asiento n.º 3586/B, Número de registro comercial 31333532 (en adelante, "ESET" o el "Proveedor") y Usted, persona física o jurídica (en adelante, "Usted" o el "Usuario final"), tiene derecho a utilizar el Software definido en el Artículo 1 del presente Acuerdo. El Software definido en este artículo puede almacenarse en un soporte digital, enviarse mediante correo electrónico, descargarse de Internet, descargarse de servidores del Proveedor u obtenerse de otras fuentes bajo los términos y condiciones mencionados más adelante.

ESTO ES UN ACUERDO SOBRE LOS DERECHOS DEL USUARIO FINAL; NO UN CONTRATO DE COMPRA PARA ARGENTINA. El Proveedor sigue siendo el propietario de la copia del Software y del soporte físico en el que el Software se suministra en paquete comercial, así como de todas las demás copias a las que el Usuario final está autorizado a hacer en virtud de este Acuerdo.

Al hacer clic en la opción "Acepto" durante la instalación, la descarga, la copia o la utilización del Software, Usted acepta los términos y condiciones del presente Acuerdo. Si no acepta todas las disposiciones de este Acuerdo, haga clic en la opción "No acepto" de inmediato, cancele la instalación o la descarga, destruya o devuelva el Software, el soporte de instalación, la documentación adjunta y el recibo de compra al Proveedor o al punto de venta donde adquirió el Software.

USTED ACEPTA QUE LA UTILIZACIÓN DEL SOFTWARE INDICA QUE HA LEÍDO ESTE ACUERDO, QUE LO COMPRENDE Y QUE CONSIENTE OBLIGARSE POR SUS TÉRMINOS Y CONDICIONES.

1. Software. Tal como se utiliza en este Acuerdo, el término "Software" significa: (i) el programa informático que acompaña a este Acuerdo y todos sus componentes; (ii) todos los contenidos de los discos, CD-ROMs, DVDs, correos electrónicos y cualquier adjunto, u otros medios con los cuales se provee este Acuerdo, incluyendo el formulario del código objeto del software provisto en soporte digital, por medio de correo electrónico o descargado a través de la Internet; (iii) cualquier material escrito explicativo relacionado y cualquier otra documentación posible relacionada con el Software, sobre todo cualquier descripción del Software, sus especificaciones, cualquier descripción de las propiedades u operación del software, cualquier descripción del ambiente operativo en el cual se utiliza el Software, instrucciones de uso o instalación del Software o cualquier descripción del modo de uso del Software (en adelante referido como "Documentación"); (iv) copias del Software, parches para posibles errores del Software, adiciones al Software, extensiones del Software, versiones modificadas del Software y actualizaciones de los componentes del Software, si existieran, con la autorización que le da a Usted el Proveedor con arreglo al Artículo 3 de este Acuerdo. El Software será provisto exclusivamente en la forma de código objeto ejecutable.

2. Instalación, equipo y clave de licencia. El Software suministrado en un soporte digital, enviado por correo electrónico, descargado de Internet, descargado de los servidores del Proveedor u obtenido de otras fuentes requiere instalación. El Software debe instalarse en un equipo correctamente configurado que cumpla, como mínimo, con los requisitos especificados en la Documentación. La metodología de instalación se describe en la Documentación. No puede haber ningún programa informático ni Hardware que pudiera afectar al Software

instalado en el equipo en el que instala el Software. El equipo hace referencia al Hardware que incluye, pero no se limita, a equipos personales, equipos portátiles, estaciones de trabajo, equipos de bolsillo, teléfonos inteligentes, dispositivos electrónicos portátiles o cualquier otro dispositivo para el que se diseñe el Software y en el que vaya a instalarse y/o utilizarse. La clave de licencia se refiere a una secuencia única de símbolos, letras números o caracteres especiales que se le brinda al Usuario final para permitirle el uso del Software de manera legal, así como de una versión específica de este o para brindarle una extensión de los términos de la Licencia en conformidad con el presente Acuerdo.

3. **Licencia.** Siempre que haya aceptado los términos de este Acuerdo y cumpla con todos los términos y condiciones aquí especificados, el Proveedor le concederá los siguientes derechos (en adelante, la "Licencia"):

a) **Instalación y uso.** Usted tendrá el derecho no exclusivo y no transferible de instalar el Software en el disco rígido de un equipo o soporte similar para un almacenamiento permanente de datos, instalar y almacenar el Software en la memoria de un sistema informático e implementar, almacenar y mostrar el Software.

b) **Disposición sobre la cantidad de licencias.** El derecho a utilizar el Software estará sujeto a la cantidad de Usuarios finales. Un "Usuario final" se refiere a lo siguiente: (i) instalación del Software en un sistema informático, o (ii) si el alcance de una licencia está vinculado a la cantidad de buzones de correo, un Usuario final se referirá a un usuario informático que acepta correo electrónico a través de un Agente de usuario de correo (en adelante, "AUC"). Si un AUC acepta el correo electrónico y lo distribuye posteriormente en forma automática a varios usuarios, la cantidad de Usuarios finales se determinará conforme a la cantidad real de usuarios para los que se distribuyó el correo electrónico. Si un servidor de correo cumple la función de una pasarela de correo, la cantidad de Usuarios finales será equivalente a la cantidad de usuarios de servidores de correo a los que dicha pasarela presta servicios. Si se envía una cantidad no especificada de direcciones de correo electrónico (por ejemplo, con alias) a un usuario y el usuario las acepta, y el cliente no distribuye automáticamente los mensajes a más usuarios, se requiere la Licencia únicamente para un equipo. No debe usar la misma Licencia en más de un equipo al mismo tiempo. El Usuario final tiene el derecho de ingresar la clave de licencia para acceder al Software solo en la medida en que utilice el Software en conformidad con las limitaciones que surgen de la cantidad de Licencias otorgadas por el Proveedor. Se considera que la clave de Licencia es confidencial. No puede compartirla con terceros ni puede permitirles que la utilicen a menos que el presente Acuerdo o el Proveedor indique lo contrario. Si su clave de Licencia se encuentra en riesgo notifique al Proveedor de inmediato.

c) **Business Edition.** Para usar el Software en servidores de correo, pasarelas de correo, puertas de enlace de correo o puertas de enlace de Internet, deberá adquirir la versión Business Edition del Software.

d) **Plazo de duración la Licencia.** El derecho a usar el Software tendrá un límite de tiempo.

e) **Software de OEM.** El Software de OEM estará limitado al equipo con el cual lo adquirió. No puede transferirse a otro equipo.

f) **Software NFR y versión de prueba.** Al Software clasificado como "No apto para la reventa", "NFR" o "Versión de prueba" no se le podrá asignar un pago y puede usarse únicamente para hacer demostraciones o evaluar las características del Software.

g) **Rescisión de la Licencia.** La Licencia se rescindirán automáticamente al finalizar el período para el cual fue otorgada. Si Usted no cumple con alguna de las disposiciones de este Acuerdo, el Proveedor tendrá el derecho de anular el Acuerdo, sin perjuicio de cualquier derecho o recurso judicial disponible para el Proveedor en dichas eventualidades. En el caso de cancelación de la Licencia, Usted deberá borrar, destruir o devolver de inmediato por su propia cuenta el Software y todas las copias de seguridad a ESET o al punto de venta donde obtuvo el Software. Tras la finalización de la Licencia, el Proveedor podrá cancelar el derecho del Usuario Final a utilizar las funciones del Software que requieran conexión a los servidores del Proveedor o de terceros.

4. Funciones con recopilación de información y requisitos para la conexión a Internet. Para que funcione de manera correcta, el Software requiere conexión a Internet y debe conectarse a intervalos regulares a los servidores del Proveedor o de terceros y debe recopilar información en conformidad con la Política de Privacidad. La conexión a Internet y la recopilación de datos son necesarias para llevar a cabo las siguientes funciones del Software:

a) **Actualizaciones del Software.** El Proveedor tendrá el derecho de lanzar actualizaciones del Software oportunamente (en adelante, “Actualizaciones”), pero no tiene la obligación de suministrar actualizaciones. Esta función se encuentra habilitada en la configuración estándar del Software, por lo que las Actualizaciones se instalan en forma automática, a menos que el Usuario final haya deshabilitado la instalación automática de las Actualizaciones. A fin de que se suministren las Actualizaciones, es necesario llevar a cabo la verificación de la autenticidad de la Licencia, que incluye información relacionada con el equipo y/o con la plataforma en la que se instale el Software en conformidad con la Política de Privacidad.

b) Envío de infiltraciones e información al Proveedor. El Software contiene funciones que reúnen muestras de virus informáticos, otros programas informáticos dañinos y objetos sospechosos, problemáticos, potencialmente no deseados o potencialmente no seguros como archivos, URL, paquetes de IP y marcos de Ethernet (en adelante denominados “Infiltraciones”) y luego los envía al Proveedor, incluidas, entre otras, la información sobre el proceso de instalación, el equipo o la plataforma en los cuales se instala el Software y la información sobre las operaciones y la funcionalidad del Software (en adelante referida como “Información”). La Información y las Infiltraciones pueden contener datos (incluidos datos personales obtenidos aleatoriamente o accidentalmente) sobre el Usuario Final u otros usuarios del equipo en el cual se encuentra instalado el Software, y archivos afectados por Infiltraciones con metadatos asociados. La Información y las Infiltraciones pueden ser recopiladas por las siguientes funciones del Software:

i. La función Sistema de reputación de LiveGride incluye la recopilación y el envío de hashes de una vía relacionados a Infiltraciones al Proveedor. Esta función se activa con la configuración estándar del Software.

ii. La función del sistema de comentarios de LiveGrid es recopilar información acerca de las infiltraciones con metadatos relacionados para enviársela al Proveedor.

El proveedor solo debe hacer uso de la información y de las infiltraciones que recibe para analizar y para investigar las infiltraciones, para mejorar el Software y el proceso de verificación de la autenticidad de la Licencia. Asimismo, debe tomar las medidas correspondientes para garantizar la seguridad de las infiltraciones y de la información que recibe. Si se activa esta función del Software, el Proveedor deberá recopilar y procesar las infiltraciones y la información tal como se especifica en la Política de Privacidad y en conformidad con las normas legales vigentes. Puede desactivar estas funciones en cualquier momento.

A los efectos de este Acuerdo, es necesario recopilar, procesar y almacenar información que permita al Proveedor identificarlo en conformidad con la Política de Privacidad. Por medio del presente, reconoce que el Proveedor utiliza sus propios medios para verificar si Usted hace uso del Software de acuerdo con las disposiciones del Acuerdo. Asimismo, reconoce que, a los efectos de este Acuerdo, es necesario que su información se transfiera durante las comunicaciones entre el Software y los sistemas informáticos del Proveedor o de sus socios comerciales como parte de la red de distribución y soporte del Proveedor a fin de garantizar la funcionalidad del Software, de autorizar el uso del Software y proteger los derechos del Proveedor.

Tras la finalización de este Acuerdo, el Proveedor o cualquiera de sus socios comerciales tendrán el derecho de transferir, procesar y almacenar datos esenciales que lo identifiquen, con el propósito de realizar la facturación y para la ejecución del presente Acuerdo y para transmitir notificaciones a su equipo. Por medio del presente, Usted acepta recibir notificaciones y mensajes que incluye, pero que no se limitan a, información relacionada con el marketing.

Los detalles sobre la privacidad, la protección de la información personal y sus derechos como parte interesada

pueden encontrarse en la Política de Privacidad, disponible en el sitio web del Proveedor y a la que se puede acceder de manera directa desde el proceso de instalación. También puede acceder a ella desde la sección de ayuda del Software.

5. Ejercicio de los derechos del Usuario final. Debe ejercer los derechos del Usuario final en persona o a través de sus empleados. Tiene derecho a utilizar el Software solamente para asegurar sus operaciones y proteger los sistemas informáticos para los que ha obtenido una Licencia.

6. Restricciones de los derechos. No puede copiar, distribuir, extraer componentes o crear versiones derivadas del Software. Al usar el Software, Usted tiene la obligación de cumplir con las siguientes restricciones:

a) Puede crear una copia del Software en un soporte de almacenamiento permanente de datos como una copia de seguridad para archivar, siempre que su copia de seguridad para archivar no esté instalada ni se utilice en ningún equipo. Cualquier otra copia que realice del Software constituirá un incumplimiento de este Acuerdo.

b) No puede utilizar, modificar, traducir ni reproducir el Software, o transferir los derechos de su uso o copias realizadas del Software de ninguna otra forma a lo establecido en este Acuerdo.

c) No puede vender, sublicenciar, arrendar o alquilar el Software, ni usarlo para suministrar servicios comerciales.

d) No puede aplicar técnicas de ingeniería inversa, descompilar o desmontar el Software, ni intentar obtener el código fuente del Software de ninguna otra forma, salvo en la medida en que esta restricción esté explícitamente prohibida por la ley.

e) Usted acepta que solo usará el Software de forma que se cumplan todas las leyes aplicables en la jurisdicción en la que lo utilice, incluyendo, pero sin limitarse a, las restricciones aplicables relacionadas con el copyright y otros derechos de propiedad intelectual.

f) Usted acepta que solamente usará el Software y sus funciones de una manera que no limite las posibilidades de otros Usuarios finales para acceder a estos servicios. El Proveedor se reserva el derecho de limitar el alcance los servicios proporcionados a Usuarios finales individuales, para activar el uso de los servicios por parte de la mayor cantidad posible de Usuarios finales. La limitación del alcance de los servicios también significará la terminación completa de la posibilidad de usar cualquiera de las funciones del Software y la eliminación de los Datos y de la información de los servidores de los Proveedores o de los servidores de terceros relacionados con una función específica del Software.

g) Usted acepta no ejercer ninguna actividad que implique el uso de la clave de Licencia de manera contraria a los términos de este Acuerdo ni que implique proporcionar la clave de Licencia a personas que no estén autorizadas a hacer uso del Software, como la transferencia de la clave de Licencia usada o no. en cualquier forma, así como la reproducción no autorizada, o la distribución de claves de Licencia duplicadas o generadas. Asimismo, no utilizará el Software como resultado del uso de una clave de Licencia obtenida de una fuente que no sea el Proveedor.

7. Copyright. El Software y todos los derechos, incluyendo, pero sin limitarse a, los derechos de propiedad y los derechos de propiedad intelectual, son propiedad de ESET y/o sus licenciatarios. Están protegidos por las disposiciones de tratados internacionales y por todas las demás leyes nacionales aplicables del país en el que se utiliza el Software. La estructura, la organización y el código del Software son valiosos secretos comerciales e información confidencial de ESET y/o sus licenciatarios. No puede copiar el Software, a excepción de lo especificado en el artículo 6 (a). Todas las copias que este Acuerdo le permita hacer deberán incluir el mismo copyright y los demás avisos legales de propiedad que aparezcan en el Software. Si aplica técnicas de ingeniería inversa, descompila o desmonta el Software, o intenta obtener el código fuente del Software de alguna otra forma, en incumplimiento de las disposiciones de este Acuerdo, por este medio Usted acepta que toda la información obtenida de ese modo se considerará automática e irrevocablemente transferida al Proveedor o poseída por el Proveedor de forma completa desde el momento de su origen, más allá de los derechos del

Proveedor en relación con el incumplimiento de este Acuerdo.

8. Reserva de derechos. Por este medio, el Proveedor se reserva todos los derechos del Software, excepto por los derechos concedidos expresamente bajo los términos de este Acuerdo a Usted como el Usuario final del Software.

9. Versiones en varios idiomas, software en medios duales, varias copias. En caso de que el Software sea compatible con varias plataformas o idiomas, o si Usted obtuvo varias copias del Software, solo puede usar el Software para la cantidad de sistemas informáticos y para las versiones correspondientes a la Licencia adquirida. No puede vender, arrendar, alquilar, sublicenciar, prestar o transferir ninguna versión o copias del Software no utilizado por Usted.

10. Comienzo y rescisión del Acuerdo. Este Acuerdo es efectivo desde la fecha en que Usted acepta los términos de la Licencia. Puede poner fin a este Acuerdo en cualquier momento. Para ello, desinstale, destruya o devuelva permanentemente y por cuenta propia el Software, todas las copias de seguridad, y todos los materiales relacionados suministrados por el Proveedor o sus socios comerciales. Más allá de la forma de rescisión de este Acuerdo, las disposiciones de los artículos 7, 8, 11, 13, 19 y 21 seguirán siendo aplicables por tiempo ilimitado.

11. DECLARACIONES DEL USUARIO FINAL. COMO USUARIO FINAL, USTED RECONOCE QUE EL SOFTWARE SE SUMINISTRA EN UNA CONDICIÓN "TAL CUAL ES", SIN UNA GARANTÍA EXPRESA O IMPLÍCITA DE NINGÚN TIPO Y HASTA EL ALCANCE MÁXIMO PERMITIDO POR LAS LEYES APLICABLES. NI EL PROVEEDOR, SUS LICENCIATARIOS, SUS AFILIADOS NI LOS TITULARES DEL COPYRIGHT PUEDEN HACER NINGUNA REPRESENTACIÓN O GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS DE COMERCIABILIDAD O ADECUACIÓN PARA UN FIN ESPECÍFICO O GARANTÍAS DE QUE EL SOFTWARE NO INFRINGIRÁ UNA PATENTE, DERECHOS DE PROPIEDAD INTELECTUAL, MARCAS COMERCIALES U OTROS DERECHOS. NO EXISTE NINGUNA GARANTÍA DEL PROVEEDOR NI DE NINGUNA OTRA PARTE DE QUE LAS FUNCIONES CONTENIDAS EN EL SOFTWARE CUMPLIRÁN CON SUS REQUISITOS O DE QUE LA OPERACIÓN DEL SOFTWARE SERÁ ININTERRUMPIDA O ESTARÁ LIBRE DE ERRORES. USTED ASUME TODA LA RESPONSABILIDAD Y EL RIESGO POR LA ELECCIÓN DEL SOFTWARE PARA LOGRAR SUS RESULTADOS DESEADOS Y POR LA INSTALACIÓN, EL USO Y LOS RESULTADOS QUE OBTENGA DEL MISMO.

12. Sin más obligaciones. Este Acuerdo no crea obligaciones del lado del Proveedor y sus licenciatarios, excepto las obligaciones específicamente indicadas en este Acuerdo.

13. LIMITACIÓN DE RESPONSABILIDAD. HASTA EL ALCANCE MÁXIMO PERMITIDO POR LAS LEYES APLICABLES, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O SUS LICENCIATARIOS SERÁN RESPONSABLES DE PÉRDIDAS DE BENEFICIOS, INGRESOS O VENTAS O DE PÉRDIDAS DE DATOS O COSTES SOPORTADOS PARA OBTENER PRODUCTOS O SERVICIOS DE SUSTITUCIÓN, DE DAÑOS A LA PROPIEDAD, DAÑOS PERSONALES, INTERRUPCIÓN DEL NEGOCIO, PÉRDIDA DE INFORMACIÓN COMERCIAL O DE DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, ACCIDENTALES, ECONÓMICOS, DE COBERTURA, CRIMINALES, ESPECIALES O SUCESIVOS CAUSADOS DE CUALQUIER MODO, YA SEA A CAUSA DE UN CONTRATO, AGRAVIO, NEGLIGENCIA U OTRO HECHO QUE ESTABLEZCA LA OCURRENCIA DE RESPONSABILIDAD, SOPORTADOS DEBIDO AL USO O A LA INCAPACIDAD DE USO DEL SOFTWARE, INCLUSO EN EL CASO DE QUE EL PROVEEDOR, SUS LICENCIATARIOS O SUS AFILIADOS HAYAN SIDO NOTIFICADOS SOBRE LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y JURISDICIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR LA LIMITACIÓN DE RESPONSABILIDAD, EN DICHOS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR, SUS EMPLEADOS, LICENCIATARIOS O AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR LA LICENCIA.

14. Nada de lo contenido en este Acuerdo perjudicará los derechos estatutarios de ninguna parte que actúe en calidad de consumidor si infringe dicho Acuerdo.

15. Soporte técnico. ESET o los terceros autorizados por ESET suministrarán soporte técnico a discreción propia,

sin ninguna garantía ni declaración. El Usuario final deberá crear una copia de seguridad de todos los datos existentes, software y prestaciones de los programas en forma previa al suministro de soporte técnico. ESET y/o los terceros autorizados por ESET no pueden aceptar la responsabilidad por el daño o pérdida de datos, propiedad, software o hardware, o pérdida de beneficios debido al suministro de soporte técnico. ESET y/o los terceros autorizados por ESET se reservan el derecho de decidir si la solución del problema excede el alcance del soporte técnico. ESET se reserva el derecho de rechazar, suspender o dar por finalizado el suministro de soporte técnico a discreción propia. Se puede solicitar información sobre la Licencia y cualquier otro tipo de información a fin de brindar soporte técnico conforme a la Política de Privacidad.

16. Transferencia de la Licencia. El Software puede transferirse de un sistema informático a otro, a menos que esta acción infrinja los términos del presente Acuerdo. Si no infringe los términos del Acuerdo, el Usuario final solamente tendrá derecho a transferir en forma permanente la Licencia y todos los derechos derivados de este Acuerdo a otro Usuario final con el consentimiento del Proveedor, sujeto a las siguientes condiciones: (i) que el Usuario final original no se quede con ninguna copia del Software; (ii) que la transferencia de los derechos sea directa, es decir, del Usuario final original al nuevo Usuario final; (iii) que el nuevo Usuario final asuma todos los derechos y obligaciones pertinentes al Usuario final original bajo los términos de este Acuerdo; (iv) que el Usuario final original le proporcione al nuevo Usuario final la Documentación que habilita la verificación de la autenticidad del Software, como se especifica en el artículo 17.

17. Verificación de la autenticidad del Software. El Usuario final puede demostrar su derecho a usar el Software en una de las siguientes maneras: (i) a través de un certificado de licencia emitido por el Proveedor o por un tercero designado por el Proveedor; (ii) a través de un acuerdo de licencia por escrito, en caso de haberse establecido dicho acuerdo; (iii) a través de la presentación de un correo electrónico enviado por el Proveedor donde se incluyan los detalles de la Licencia (nombre de usuario y contraseña). Se puede solicitar información sobre la Licencia y datos sobre el Usuario final a para llevar a cabo la verificación de la autenticidad del Software conforme a la Política de Privacidad.

18. Licencias para autoridades públicas y el gobierno de los Estados Unidos. Se deberá suministrar el Software a las autoridades públicas, incluyendo el gobierno argentino, con los derechos de la Licencia y las restricciones descritas en este Acuerdo.

19. Cumplimiento del control comercial.

a) Usted no podrá, ya sea directa o indirectamente, exportar, reexportar o transferir el Software, o de alguna otra forma ponerlo a disposición de ninguna persona, o utilizarlo de ninguna manera, o participar de ningún acto, que pueda ocasionar que ESET o sus compañías controladoras, sus empresas subsidiarias y las subsidiarias de cualquiera de sus compañías controladoras, así como también las entidades controladas por sus compañías controladoras (en adelante, "Afiliadas") violen, o queden sujetas a las consecuencias negativas de las Leyes de Control Comercial, las cuales incluyen

i. toda ley que controle, restrinja o imponga requisitos de licencia a la exportación, reexportación o transferencia de productos, software, tecnología o servicios, establecida o adoptada por cualquier gobierno, estado o autoridad reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados Miembro, o cualquier país donde deban cumplirse las obligaciones conforme al Acuerdo, o donde ESET o cualquiera de sus Afiliadas operen o estén constituidas (en adelante, "Leyes de Control de Exportaciones") y

ii. cualquier sanción, restricción, embargo, prohibición de exportación o importación, prohibición de transferencia de fondos o activos o prohibición de prestación de servicios, ya sea de índole económica, financiera, comercial o de otro tipo, o toda medida equivalente impuesta por cualquier gobierno, estado o autoridad reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados Miembro, o cualquier país donde deban cumplirse las obligaciones conforme al Acuerdo, o donde ESET o cualquiera de sus Afiliadas operen o estén constituidas (en adelante, "Normas sancionadoras").

b) ESET tendrá el derecho de suspender sus obligaciones conforme a estos Términos o terminar el Acuerdo, con efecto inmediato, en los siguientes casos:

i. ESET determina que, en su razonable opinión, el Usuario ha violado o podría violar la disposición del Artículo 19.a del Acuerdo; o

ii. el Usuario final o el Software quedan sujetos a las Leyes de Control Comercial y, en consecuencia, ESET determina que, en su razonable opinión, el cumplimiento continuo de sus obligaciones conforme al Acuerdo podría ocasionar que ESET o sus Afiliadas incurriesen en la violación de las Leyes de Control Comercial o quedasen sujetas a las consecuencias negativas de estas.

c) Ninguna de las estipulaciones del Acuerdo tiene por objeto inducir o exigir, ni debe interpretarse como una intención de inducir o exigir a ninguna de las partes actuar o abstenerse de actuar (o acordar actuar o abstenerse de actuar) de ninguna manera que resulte inconsistente con las Leyes de Control Comercial aplicables, o se encuentre penalizada o prohibida por estas.

20. **Avisos.** Todos los avisos, la devolución del Software y la Documentación deben enviarse a: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

21. **Legislación aplicable.** Este Acuerdo se registrará e interpretará conforme a la legislación de la República Eslovaca. En el presente Acuerdo, el Usuario final y el Proveedor aceptan que los principios del conflicto de leyes y la Convención de las Naciones Unidas sobre los Contratos de Venta Internacional de Bienes no serán aplicables. Acepta expresamente que cualquier disputa o demanda derivada del presente Acuerdo con respecto al Proveedor o relativa al uso del Software deberá resolverse por el Tribunal del Distrito de Bratislava I., Eslovaquia; asimismo, Usted acepta expresamente el ejercicio de la jurisdicción del Tribunal mencionado.

22. **Disposiciones generales.** Si alguna disposición de este Acuerdo no es válida o aplicable, no afectará la validez de las demás disposiciones del Acuerdo, que seguirán siendo válidas y ejecutables bajo las condiciones aquí estipuladas. En caso de existir diferencias entre las versiones idiomáticas de este Acuerdo, prevalecerá el texto en lengua inglesa. Las revisiones de este Acuerdo pueden realizarse únicamente por escrito y deberán estar firmadas ya sea por un representante autorizado por el Proveedor o por una persona expresamente autorizada para actuar en su nombre según lo establezcan las disposiciones de un poder notarial.

Este es el acuerdo entero entre el proveedor y Usted relacionado con el Software y reemplaza a cualquier representación, discusión, garantía, comunicación o publicidad previa relacionadas con el Software.

EULA ID: BUS-ECOS-20-01

Data Processing Agreement

De acuerdo con los requisitos de la Regulación (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016, sobre la protección de las personas físicas en lo que respecta al procesamiento de datos personales y a la libre circulación de estos datos, la cual deroga la Directiva 95/46/CE (en adelante denominada "RGPD"), el Proveedor (en adelante denominado el "Procesador") y el Usuario (en adelante denominado el "Controlador") celebran este contrato de procesamiento de datos con el objetivo de definir los términos y las condiciones del procesamiento de datos personales y el modo de protección, así como también, para definir los otros derechos y obligaciones de ambas partes en relación con el procesamiento de datos personales de los titulares de datos, realizado en representación del Controlador, en el marco del cumplimiento del objeto de estos Términos, como contrato principal.

1. **Procesamiento de datos personales.** Los servicios provistos en cumplimiento de estos Términos incluyen el procesamiento de información relacionada con un individuo identificado o identificable, enumerada en la [Política](#)

[de privacidad](#) (en adelante denominada "Datos personales").

2. Autorización. El Controlador autoriza al Procesador a procesar datos personales, lo cual incluye lo siguiente:

(i) "propósito del procesamiento" significa la provisión de servicios de conformidad con estos Términos; El Procesador solo puede procesar los Datos personales en nombre del Controlador en relación con la prestación de servicios solicitada por el Controlador. Toda la información recopilada con fines adicionales se procesa fuera de la relación contractual Controlador-Procesador.

(ii) "periodo de procesamiento" significa el periodo que comienza con el inicio de la cooperación, de conformidad con estos Términos, hasta la finalización de los servicios;

(iii) alcance y categorías de los datos personales. Los Servicios están previstos solo para el procesamiento de datos personales generales. Sin embargo, el Controlador es el único responsable de la determinación del alcance de los datos personales.

(iv) "titular de datos" significa un individuo que actúa como usuario autorizado de los dispositivos del Controlador;

(v) "operaciones de procesamiento" significa todas y cada una de las operaciones necesarias a los efectos del procesamiento;

(iv) "instrucciones documentadas" significa las instrucciones descritas en estos Términos, los anexos, la política de privacidad y la documentación del servicio. El Controlador será responsable de la admisibilidad legal de procesamiento de los Datos personales por parte del Procesador en relación con las correspondientes disposiciones aplicables de la ley de protección de datos.

3. Obligaciones del Procesador. El Procesador tiene las siguientes obligaciones:

(i) procesar los Datos personales solo de acuerdo con las instrucciones documentadas y con el fin definido en los Términos, sus Anexos, la Política de privacidad y la documentación de servicio;

Indicar a las personas autorizadas para procesar los Datos personales (en lo sucesivo, "Personas autorizadas") sus derechos y deberes de conformidad con la GDPR, su responsabilidad en caso de incumplimiento de los deberes y garantizar que las Personas autorizadas para procesar los Datos personales se hayan comprometido a guardar la confidencialidad y a acatar las instrucciones documentadas.

(iii) implementar y seguir las medidas descritas en los Términos, sus Anexos, la Política de privacidad y la documentación de servicio;

(iv) ayudar al Controlador a responder las solicitudes de los Interesados en relación con sus derechos. El Procesador no corregirá, eliminará ni restringirá el procesamiento de los Datos personales sin las instrucciones del Controlador; Todas las solicitudes del Interesado en relación con los Datos personales procesados en nombre del Controlador se enviarán a este sin demora;

(v) ayudar al Controlador en la notificación de una filtración de Datos personales a la autoridad supervisora y al Interesado; El Procesador notificará al Controlador toda infracción del procesamiento de datos personales o de la seguridad de los datos personales inmediatamente después de su descubrimiento. El Procesador cooperará en la medida de lo razonable en la investigación y la corrección de dicha infracción y adoptará medidas razonables para limitar las consecuencias negativas ulteriores.

(vi) a discreción del Controlador, eliminar o devolver todos los Datos personales al Controlador una vez que finalice el Periodo de procesamiento. El Controlador se compromete a informar al Procesador su decisión en un plazo de diez (10) días después de la finalización del Período de procesamiento. Esta disposición no afectará al derecho del Procesador a conservar los Datos personales en la medida necesaria para fines de archivo por

motivos de interés público, investigación científica, estadísticas o el establecimiento, el ejercicio o la defensa de reclamos legales.

(vii) mantener un registro actualizado de todas las categorías de las actividades de procesamiento que ha realizado en representación del Controlador;

(viii) presentar toda la información necesaria para demostrar el cumplimiento como parte de los Términos, sus Anexos, la Política de privacidad y la documentación de servicio a disposición del Controlador. En caso de auditoría o control del procesamiento de Datos personales por parte del Controlador, este estará obligado a informar al Procesador por escrito al menos diez (30) días antes de la auditoría o control previstos.

4. Contratación de otro Procesador. El Procesador tiene derecho a contratar a otro procesador para que realice actividades de procesamiento específicas, como la provisión de almacenamiento e infraestructura en la nube para el servicio, de conformidad con los Términos, sus Anexos, la Política de privacidad y la documentación de servicio. Actualmente, Microsoft ofrece almacenamiento e infraestructura en la nube como parte del servicio en la nube de Azure. Incluso en este caso, el Procesador seguirá siendo el único punto de contacto y el responsable del cumplimiento. El Procesador se compromete a informar al Controlador toda adición o sustitución de otro Procesador a los efectos de la posibilidad de oposición a dicho cambio.

5. Ámbito de procesamiento. El Procesador garantiza que el procesamiento se llevará a cabo en el Espacio Económico Europeo o en un país designado como seguro por la Comisión Europea, en función de la decisión del Controlador. Las Disposiciones contractuales estándar se aplicarán en el caso de que se produzcan transferencias y actividades de procesamiento fuera del Espacio Económico Europeo o de un país designado como seguro por la Comisión Europea, a solicitud del Controlador.

6. Seguridad. El Procesador posee la certificación de la norma ISO 27001:2013 y adopta el marco de la norma ISO 27001 con el fin de implementar una estrategia de seguridad basada en la defensa en capas, al momento de aplicar los controles de seguridad en la capa de la red, los sistemas operativos, las bases de datos, las aplicaciones, y los procesos operativos y de personal. El cumplimiento de los requisitos contractuales y regulatorios se evalúa y se revisa de manera periódica, al igual que otras infraestructuras y otros operaciones del Procesador. Además, se toman las medidas necesarias para garantizar el cumplimiento continuo. El Procesador ha organizado la seguridad de los datos con el Sistema de Gestión de la Seguridad de la Información (SGSI), en función de la norma ISO 27001. La documentación sobre seguridad incluye, principalmente, políticas sobre seguridad de la información, protección física y seguridad del equipamiento, gestión de incidentes, gestión de pérdida de datos e incidentes de seguridad, etc.

7. Medidas técnicas y organizativas. El Procesador protegerá los Datos personales de daños y destrucción fortuitos e ilícitos, pérdida fortuita, cambios, acceso no autorizado y divulgación. En tal sentido, el Procesador adoptará las medidas técnicas y organizativas adecuadas al modo de procesamiento y al riesgo que presente el procesamiento para los derechos de los Interesados, de conformidad con los requisitos de la GDPR. En la Política de seguridad, se incluye una descripción detallada de las medidas técnicas y organizativas.

8. Información de contacto del Procesador. Todas las notificaciones, las solicitudes, los pedidos y otras comunicaciones relativas a la protección de los datos personales deben dirigirse a ESET, spol. s.r.o., con los siguientes datos: Data Protection Officer, Einsteinova 24, 85101 Bratislava, Slovak Republic, email: dpo@eset.sk.

Standard Contractual Clauses

SECTION I

Clause 1 Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE ONE: Transfer controller to controller

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

- (i) where it has obtained the data subject's prior consent;
- (ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

- (i) of its identity and contact details;
- (ii) of the categories of personal data processed;
- (iii) of the right to obtain a copy of these Clauses;
- (iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation (2) of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions

and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (3) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter.

The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter (5).

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of

processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (6) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.
- (c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
- (d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
- (e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be

carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data (7), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9 Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (9) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. (10) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in

Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11 Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each

other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data

importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY

PUBLIC AUTHORITIES

Clause 14 Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination— including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify

appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:; if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data

exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law as defined in Terms.

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law as defined in Terms.

Clause 18 Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts as defined in Terms.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts as defined in Terms.

APPENDIX

EXPLANATORY NOTE: It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Controller as defined in Data Processing Agreement
2. Processor as defined in Data Processing Agreement

(based on the flow of data)

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

1. Controller as defined in Data Processing Agreement
2. Processor as defined in Data Processing Agreement

(based on the flow of data)

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred: As defined in Data Processing Agreement.

Categories of personal data transferred: As defined in Data Processing Agreement and Privacy Policy.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions

(including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: As defined in Data Processing Agreement and Privacy Policy.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Continuous basis.

Nature of the processing: Automated.

Purpose(s) of the data transfer and further processing: Provision of service as defined in Terms, its Annexes, Privacy Policy, and service documentation.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: As defined in Data Processing Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: As defined in Data Processing Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13: As defined in Privacy Policy

ANNEX II TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE: The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons: As defined in Security Policy

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE: This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors: As defined in Data Processing Agreement

References:

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(2) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

(3) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(4) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(5) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

(6) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

(7) This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

(8) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(9) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(10) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(11) The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(12) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Política de privacidad

Vigente a partir del 21.º de marzo de 2023 | [Consulte una versión anterior de la Política de privacidad](#) | [Comparar cambios](#)

La protección de los datos personales reviste especial importancia para ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, Slovak Republic, inscrita en el Registro comercial del Tribunal de Distrito de Bratislava I, Sección Sro, Registro N.º 3586/B, Número de registro de empresa: 31333532 como controlador de datos (“ESET” o “Nosotros”). Queremos cumplir con el requisito de transparencia de acuerdo con el Reglamento General de Protección de Datos de la Unión Europea (“RGPD”). A fin de cumplir con el objetivo, publicamos la presente Política de privacidad con el único propósito de informar a nuestros clientes (“Usuario final” o “Usted”), en carácter de interesados, acerca de los siguientes temas relativos a la protección de los datos personales:

- Fundamento jurídico para el procesamiento de datos personales.
- Intercambio y confidencialidad de los datos.
- Seguridad de los datos.
- Sus derechos como interesado.
- Procesamiento de sus datos personales.
- Información de contacto.

Fundamento jurídico para el procesamiento de datos personales

Existen solo unas pocas bases legales para el procesamiento de datos que usamos de acuerdo con el marco legislativo aplicable en relación con la protección de datos personales. En ESET, el procesamiento de datos

personales es necesario principalmente a fin de cumplir con el [Términos de uso](#) (“Términos”) con el Usuario final [Art. 6 (1) (b) del Reglamento General de Protección de Datos (RGPD)], que rige la prestación de productos o servicios de ESET, a menos que se indique algo distinto explícitamente, p. ej.:

- El fundamento jurídico del interés legítimo, conforme al Art. 6 (1) (f) del RGPD, que nos permite procesar los datos sobre cómo nuestros clientes usan nuestros Servicios y su satisfacción a fin de ofrecerles a nuestros usuarios el máximo nivel posible en protección, soporte y experiencia. Incluso la legislación aplicable reconoce el marketing como un interés legítimo. Por lo tanto, solemos confiar en este concepto cuando se trata de la comunicación de marketing con nuestros clientes.
- El consentimiento, conforme al Art. 6 (1) (a) del RGPD, que podemos solicitarle a Usted en situaciones específicas en las que consideramos que este fundamento jurídico es el más adecuado o si lo exige la ley.
- El cumplimiento de una obligación legal, conforme al Art. 6 (1) (c) del RGPD, por ejemplo, una que estipula los requisitos para la comunicación electrónica o la retención de documentos de facturación o cobranza.

Intercambio y confidencialidad de los datos

No compartimos sus datos con terceros. Sin embargo, ESET es una compañía que opera globalmente a través de entidades afiliadas o socios como parte de nuestra red de venta, servicio y soporte. La información sobre licencias, facturación y soporte técnico que procesa ESET puede ser transferida desde las entidades afiliadas o los socios o hacia ellos a fin de ejecutar el EULA, por ejemplo, para la prestación de servicios o soporte.

ESET prefiere procesar sus datos en la Unión Europea (UE). Sin embargo, según su ubicación (el uso de nuestros productos o servicios fuera de la UE) o el servicio que elija, puede que sea necesario transmitir sus datos a un país ubicado fuera de la UE. Por ejemplo, usamos servicios de terceros en conexión con la informática en la nube. En estos casos, seleccionamos cuidadosamente a nuestros proveedores de servicios y garantizamos un nivel adecuado de protección de los datos mediante medidas contractuales, técnicas y organizativas. Por regla general, pactamos las cláusulas contractuales estándar de la UE, si es necesario, con normas contractuales complementarias.

En el caso de algunos países fuera de la UE, como Reino Unido y Suiza, la UE ya ha determinado un nivel de protección de datos equivalente. Debido a este nivel de protección de datos equivalente, la transferencia de datos hacia estos países no requiere ninguna autorización ni acuerdo especial.

Nos basamos en servicios de terceros relacionados con la informática en la nube proporcionados por Microsoft como proveedor de servicios en la nube.

Seguridad de los datos

ESET implementa medidas técnicas y de organización para asegurar un nivel de seguridad apropiado ante riesgos potenciales. Hacemos todo lo posible para garantizar una continua confidencialidad, integridad, disponibilidad y resistencia de los sistemas operativos y servicios. Sin embargo, si ocurre una filtración de datos que genera un riesgo para sus derechos y libertades, estamos preparados para notificar a la autoridad supervisora pertinente, como también a los Usuarios finales afectados que actúen en carácter de interesados.

Derechos de la persona registrada

Los derechos de los Usuarios finales son importantes. Queremos informarle que cada Usuario final (de cualquier país, dentro y fuera de la Unión Europea) tiene los siguientes derechos, que ESET garantiza. Para ejercer los derechos de los interesados, puede comunicarse con nosotros a través del formulario de soporte o por correo electrónico a la siguiente dirección: dpo@eset.sk. A fin de poder identificarlo, le solicitamos la siguiente información: Nombre, dirección de correo electrónico y, de estar disponible, clave de licencia o número de cliente

y empresa de afiliación. No debe enviarnos ningún otro dato personal, como la fecha de nacimiento. Queremos señalar que, para poder procesar su solicitud, así como con fines de identificación, procesaremos sus datos personales.

Derecho a retirar el consentimiento. El derecho a retirar el consentimiento resulta aplicable únicamente cuando nuestro procesamiento requiera su consentimiento. Si procesamos sus datos personales en razón de su consentimiento, tiene derecho a retirarlo en cualquier momento sin expresión de causa. Solo podrá retirar su consentimiento con efectos para el futuro, lo que no afectará la legitimidad de los datos procesados con anterioridad.

Derecho a oponerse. El derecho a oponerse al procesamiento resulta aplicable únicamente cuando nuestro procesamiento esté basado en el interés legítimo de ESET o un tercero. Si procesamos sus datos personales en pos de un interés legítimo, Usted, como interesado, tiene derecho a oponerse, en cualquier momento, al interés legítimo que designemos y al procesamiento de sus datos personales. Solo podrá oponerse al procesamiento con efectos para el futuro, lo que no afectará la legitimidad de los datos procesados con anterioridad. Si procesamos sus datos personales con fines de marketing directo, no es necesario que exprese una causa. Esto también se aplica a la elaboración de perfiles, ya que se relaciona con el marketing directo. En todos los demás casos, le solicitamos que nos informe, de forma breve, sus quejas en contra del interés legítimo de ESET para el procesamiento de sus datos personales.

Tenga en cuenta que, en algunos casos, a pesar de que haya retirado su consentimiento, tenemos derecho a continuar procesando sus datos personales en función de algún otro fundamento jurídico, por ejemplo, para el cumplimiento de un contrato.

Derecho de acceso. En carácter de interesado, Usted tiene derecho a obtener información de los datos que almacene ESET sobre usted de forma gratuita, en cualquier momento.

Derecho a solicitar una rectificación. En caso de que procesemos de forma involuntaria datos personales incorrectos sobre Usted, tiene derecho a que se corrija esta información.

Derecho a solicitar el borrado de los datos y la restricción en el procesamiento. En carácter de interesado, Usted tiene derecho a solicitar el borrado de sus datos personales o una restricción en su procesamiento. Si procesamos sus datos personales, por ejemplo, con su consentimiento, Usted lo retira y no hay ningún otro fundamento jurídico (como un contrato), eliminaremos sus datos personales de inmediato. También eliminaremos sus datos personales en cuanto ya no sean necesarios para los fines indicados cuando finalice nuestro período de retención.

Si usamos sus datos personales únicamente con el fin de marketing directo y Usted ha retirado su consentimiento o se ha opuesto al interés legítimo subyacente de ESET, restringiremos el procesamiento de sus datos personales, lo que implicará que sus datos de contacto se incluyan en nuestra lista negra interna para evitar el contacto no solicitado. De lo contrario, sus datos personales serán eliminados.

Tenga en cuenta que podemos tener la obligación de almacenar sus datos hasta que finalicen los períodos y las obligaciones de retención determinados por el legislador o las autoridades supervisoras. La legislación eslovaca también podría determinar períodos y obligaciones de retención. A partir de su finalización, los datos correspondientes se eliminarán de forma rutinaria.

Derecho a la portabilidad de datos. Nos complace proporcionarle a Usted, en carácter de interesado, los datos personales que procese ESET en formato xls.

Derecho a presentar una queja. Como interesado, Usted tiene el derecho de presentar una queja a una autoridad supervisora en cualquier momento. ESET se encuentra sujeto a la regulación de las leyes eslovacas y Nosotros cumplimos con la ley de protección de datos como parte de la Unión Europea. La autoridad supervisora competente en materia de datos es la Oficina de Protección de Datos Personales de la República de Eslovaquia,

con sede en Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Procesamiento de sus datos personales

Los servicios provistos por ESET implementados en nuestros productos web se proporcionan bajo los Términos de Uso ("Términos"). Sin embargo, algunos de ellos pueden requerir una atención específica. Nos gustaría brindarle más detalles sobre el procesamiento de datos relacionado con el suministro de nuestros productos y servicios. Prestamos diversos servicios descritos en los [Términos](#) y la [documentación](#). Para hacer que todo funcione, necesitamos recolectar la siguiente información:

Datos de facturación y licencia. ESET recopila y procesa el nombre, la dirección de correo electrónico, la clave de licencia y, si corresponde, la dirección, la empresa de afiliación y los datos de pago para facilitar la activación de la licencia, la entrega de la clave de licencia, los recordatorios sobre caducidad, las solicitudes de soporte, la verificación de la autenticidad de la licencia, la prestación de nuestro servicio y otras notificaciones, como mensajes de marketing acordes a la legislación aplicable o Su consentimiento. ESET tiene la obligación legal de conservar la información de facturación durante un plazo de 10 años, pero la información sobre licencias se anonimiza a más tardar 12 meses después de la caducidad de la licencia.

Actualización y otras estadísticas. La información procesada comprende información relacionada con el proceso de instalación y su equipo, lo que incluye la plataforma en la que está instalado nuestro producto e información sobre las operaciones y la funcionalidad de nuestros productos, como el sistema operativo, información sobre el hardware, identificadores de instalación, identificadores de licencias, dirección IP, dirección MAC o ajustes de configuración del producto. Esta información se procesa con el fin de prestar servicios de actualización y a efectos del mantenimiento, la seguridad y la mejora de nuestra infraestructura de backend.

Esta información se encuentra separada de la información de identificación necesaria para las licencias y la facturación, ya que no requiere la identificación del Usuario final. El período de retención es de hasta cuatro años.

Sistema de reputación de **ESET LiveGrid®**. Las funciones hash unidireccionales relativas a infiltraciones se procesan a efectos del sistema de reputación de ESET LiveGrid®, que mejora la eficiencia de nuestras soluciones de protección contra malware comparando archivos analizados con una base de datos de elementos en listas blancas y negras en la nube. Durante este proceso, no se identifica al Usuario final.

Sistema de comentarios de **ESET LiveGrid®**. Muestras y metadatos sospechosos de la circulación, parte del sistema de realimentación de ESET LiveGrid®, que permite a ESET reaccionar de forma inmediata ante las necesidades de sus usuarios finales y responder a las amenazas más recientes. Nosotros dependemos de que Usted nos envíe:

- Infiltraciones como muestras potenciales de virus y otros programas malignos y sospechosos; objetos problemáticos o potencialmente no deseados o inseguros, como archivos ejecutables, mensajes de correo electrónico que haya clasificado, como correo no deseado o que nuestro producto haya marcado;
- Información relativa al uso de Internet, como dirección IP e información geográfica, paquetes IP, URL y marcos de Ethernet;
- Archivos de volcado de memoria y la información que contienen.

No necesitamos recopilar datos por fuera de este ámbito. Sin embargo, en algunas ocasiones no podemos evitarlo. Los datos recopilados accidentalmente pueden incluirse como malware y Nosotros no pretendemos que sean parte de nuestros sistemas o procesarlos para el cumplimiento de los objetivos detallados en la presente Política de privacidad.

Toda la información obtenida y procesada a través del sistema de comentarios de ESET LiveGrid® ha de utilizarse sin la identificación de Usuario final.

Soporte técnico. Se puede solicitar la información de contacto, la información de licencia y los datos incluidos en sus solicitudes de soporte para brindar asistencia. Basados en el medio que Usted eligió para comunicarse con Nosotros, podemos recopilar su correo electrónico, número de teléfono, datos de licencia, detalles del producto y descripción de su caso de asistencia. Podemos solicitarle que proporcione datos adicionales para facilitar la prestación del servicio de soporte. Los datos procesados a los fines del soporte técnico se almacenan durante cuatro años.

Tenga en cuenta que, si la persona que usa nuestros productos y servicios no es el Usuario final que ha adquirido el producto o el servicio y cerrado los Términos con nosotros (por ejemplo, un empleado del Usuario final, un familiar o una persona autorizada por el Usuario final de otra forma a usar el producto o el servicio de acuerdo con los Términos), el procesamiento de los datos se lleva a cabo en pos del interés legítimo de ESET en virtud del Artículo 6 (1) (f) del RGPD, a fin de permitir que el usuario autorizado por el Usuario final use los productos y servicios prestados por Nosotros en virtud de los Términos.

Información de contacto

Si desea ejercer su derecho como persona registrada o tiene una consulta o preocupación, envíenos un mensaje a:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk